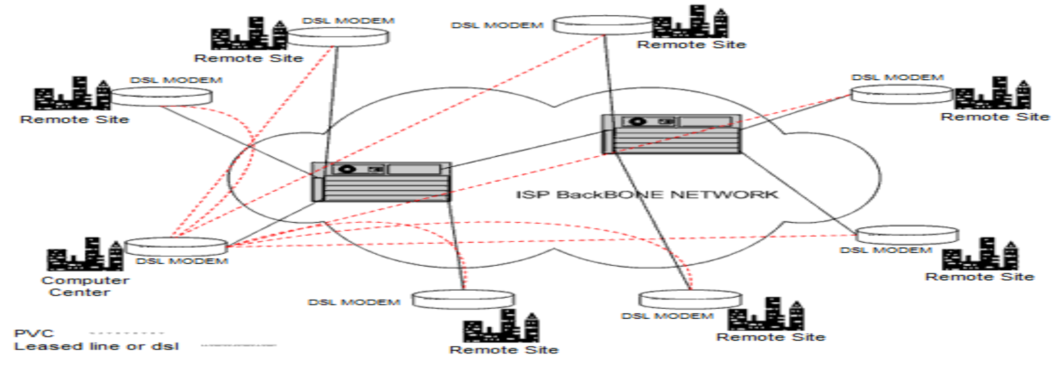
PLAN DU SOUS SAVOIR S34

A. Présentation des réseaux étendus « WAN »

I. Définitions

Un réseau WAN, d'un point de vue général, est un ensemble de liaisons reliées aux différents opérateurs, qui sont interconnectés.



Les caractéristiques principales des réseaux WAN sont :

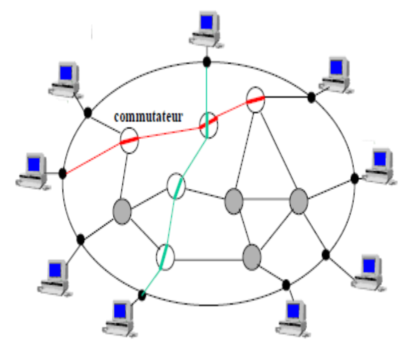
- Fonctionnent sur de vastes étendues géographiques.
- Utilisent les services d'un opérateur Télécom.
- Transportent différents types de trafic (Voix, données, vidéo).
- Axés sur les couches physiques et liaison de données du modèle OSI.

Le rôle des opérateurs Télécom est de fournir une communication bout à bout, en utilisant diverses méthodes de commutation (circuits, paquets, cellules), tout en fournissant des services.

- **La commutation de circuits :**

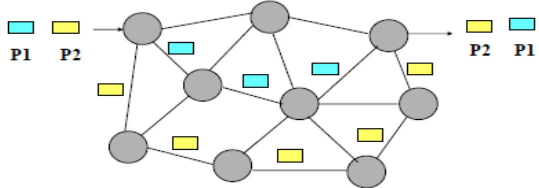
Elle est issue des techniques utilisées dans les réseaux téléphoniques (RTC).
Elle se déroule en 3 phases :

- **La connexion** : un chemin est établi entre l'appelant et l'appelé, par commutations successives. Les commutateurs ne remplissent qu'une fonction d'aiguillage. Tout se passe comme s'il n'y avait qu'une seule liaison entre les deux extrémités.
- **Le transfert :** Les données (ou la voix) sont transmises de bout en bout sur le "circuit de données".
- **La libération** : après le transfert, les ressources sont restituées au réseau de commutation, et sont disponibles pour d'autres communications.



- **La commutation de paquets :**

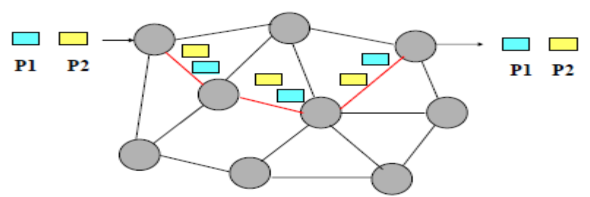
Les paquets sont transmis de nœud en nœud, au fur et à mesure que la connexion est établie, sans s'assurer que les ressources soient disponibles de bout en bout.



P1 et P2 suivent des parcours différents, et arrivent dans le désordre

- **La commutation de cellules :**

En commutation de cellules (paquets en mode connecté), un **circuit** est établi de bout en bout, avant de transférer le message, comme pour la commutation de circuits. Mais il s'agit bien de la **commutation de paquets** (le circuit est **virtuel**).



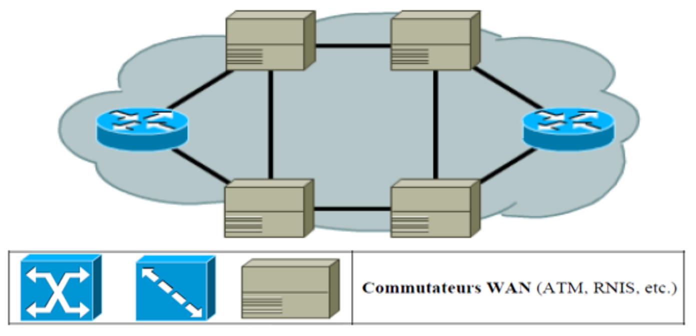
II. Equipements et dispositifs WAN

Les réseaux WAN utilisent, entre autres, les équipements suivants :

- Les routeurs sont des unités qui offrent de nombreux services pour l'interconnexion de réseaux (niveau 3 OSI) via des ports d'interface LAN et WAN. Ils permettent une grande diversité de liaisons et de sous-réseaux, à des débits différents. Ce sont des unités de réseau actives et intelligentes, capables de participer à l'administration d'un réseau. Ils fournissent des services de connectivité et leurs performances sont fiables.



- Les commutateurs WAN sont des unités de réseau multiport qui assurent les commutations du trafic de type Frame Relay ou X.25 et des services de commutation de données haut débit (SMDS : Switched Multi-megabit Data Service). Les commutateurs WAN fonctionnent généralement au niveau de la couche liaison de données du modèle OSI. La figure illustre deux routeurs situés aux extrémités d'un réseau WAN, reliés par des commutateurs WAN. Dans cet exemple, les commutateurs filtrent, acheminent et diffusent les trames selon leur adresse de destination.



Commutateurs WAN (ATM, RNIS, etc.)

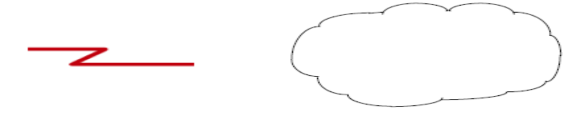
- Les modems sont des équipements qui transforment les signaux numériques en analogiques en modulant et en démodulant le signal, ce qui permet de transmettre des données sur des lignes téléphoniques à fréquence vocale. À la source, les signaux numériques sont convertis dans un format approprié pour la transmission par des unités de communication analogique. À la destination, ces signaux analogiques sont reconvertis en signaux numériques. La figure illustre une connexion simple entre deux modems sur un réseau WAN...



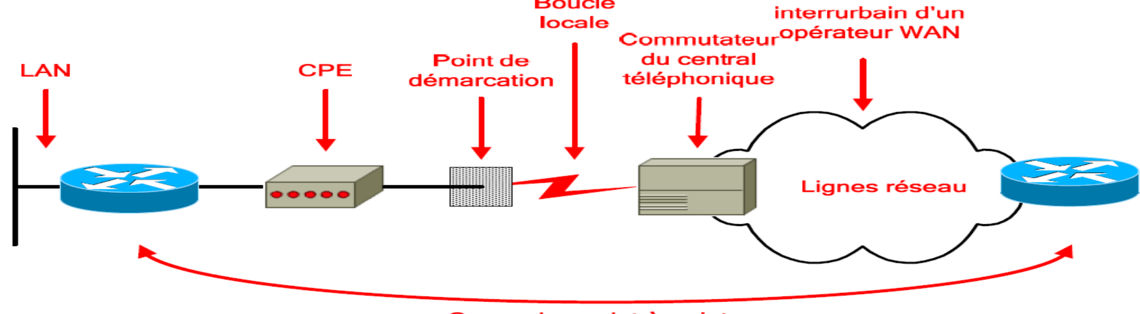
- Les serveurs de communication, qui concentrent les communications utilisateur entrantes et sortantes.



- A quoi on peut rajouter les liaisons WAN elles-mêmes qu'on symbolise par un nuage pour représenter les réseaux commutés des opérateurs ou une ligne brisée pour les liaisons point à point.



Exemple d'une liaison WAN



- **CPE** : Equipement placé dans les locaux du client, lui appartenant ou étant loué à l'opérateur (Exemple : modem).
- **Point de démarcation de service** : Démarcation entre la partie client et la partie opérateur (boucle locale). C'est à ce point que la responsabilité de chaque partie (Client et opérateur) s'arrête.
- **Boucle locale** : Partie reliant le point de démarcation de service au central téléphonique de l'opérateur.
- **Commutateur du central téléphonique** : Point de commutation le plus proche du client.
- **Réseau interurbain** : Unités et commutateur (appelés lignes réseau) situés dans le nuage de l'opérateur.

Exemples de lignes WAN et bande passante associée :

Type de ligne	Bande passante
T1	1.544 Mbits/s
E1	2.048 Mbits/s
E3	34.064 Mbits/s
T3	44.736 Mbits/s

III. Normes WAN

Les normes des réseaux WAN décrivent généralement les méthodes d'acheminement de la couche physique ainsi que la configuration exigée pour la couche liaison de donnée, notamment :

- L'adressage.
- Le contrôle de flux.
- L'encapsulation.

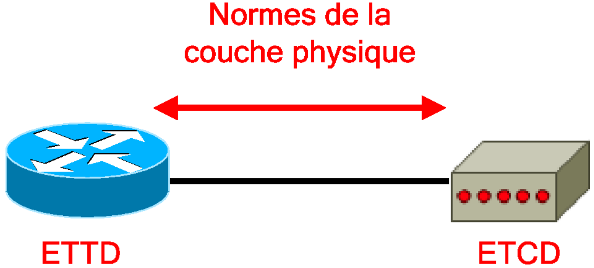
Les principaux organismes définissant et gérant les normes WAN sont :

- **UIT-T** (Union Internationale des Télécommunications - secteur de normalisation des Télécommunications), anciennement appelée **CCITT** (Comité Consultatif International Télégraphique et Téléphonique).
- **ISO** (International Standards Organization).
- **IETF** (Internet Engineering Task Force).
- **EIA** (Electrical Industries Association).
- **TIA** (Telecommunications Industry Association).

❖ Normes de la couche physique

La couche physique d'un réseau WAN décrit principalement l'interface entre l'ETTD (équipement terminal de traitement de données) et l'ETCD (équipement de terminaison de circuit de données)

- En règle générale, l'ETCD est du côté du fournisseur de services et l'ETTD est l'unité cliente à connecter au WAN.
- En Anglais ETTD se dit DTE (Data Terminal Equipment) et ETCD, DCE (Data Comunication Equipement).



Le but principal de l'ETCD est de servir d'interface entre l'ETTD et la liaison de communication WAN de l'opérateur :

- L'ETTD fournit les données de l'utilisateur (Exemple : routeur).
- L'ETCD convertit le format des données de l'utilisateur en un format acceptable par les unités du service réseau WAN (Exemple : modem, unité CSU/DSU : Channel Service Unit et Data Service Unit , TA, NT1).

❖ Normes de la couche liaison de données

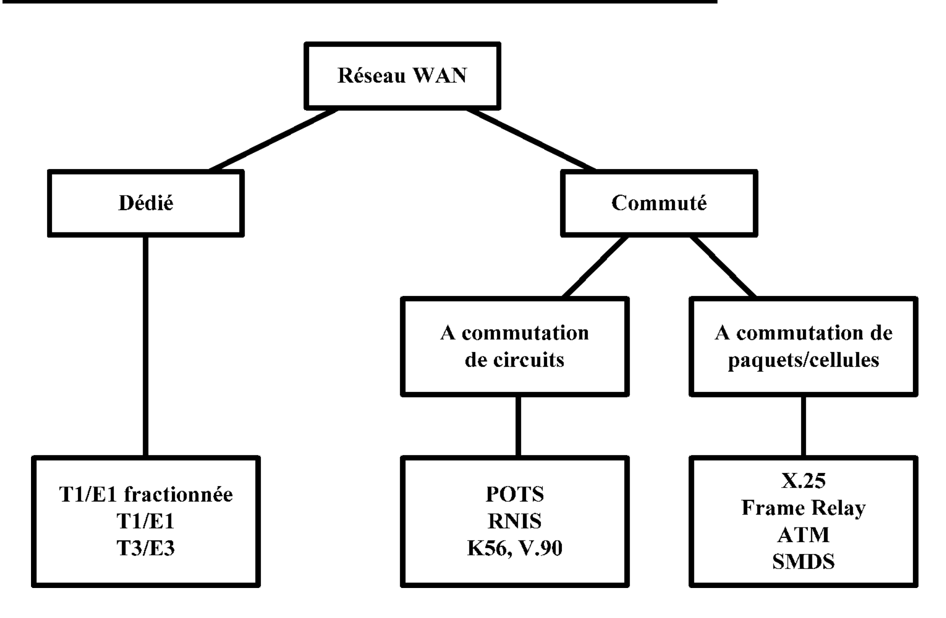
Encapsulations
(couche 2)

La couche liaison de données définit le mode d'encapsulation des données sur les réseaux WAN :

- **Frame Relay** :
  - Encapsulation simplifiée.
  - Dépourvue de mécanismes de correction des erreurs.
  - Prévu pour des unités numériques haut de gamme.
  - Transmet les données très rapidement par rapport aux autres encapsulations WAN.
  - Il existe deux variantes pour cette encapsulation, à savoir Cisco et IETF.
- **PPP** (Protocole Point-à-Point):
  - Comprend un champ identifiant le protocole de couche réseau.
  - Vérifie la qualité de la liaison au moment de l'établissement d'une connexion.
  - Gère l'authentification grâce aux protocoles PAP et CHAP.
- **RNIS** (Réseau Numérique à Intégration de Services) :
  - Ensemble de services numériques pour la voix et les données sur le réseau commuté classique.
- **LAPB** (Link Access Procedure Balanced) **:**
  - Encapsulation des paquets à la couche 2 de la pile X.25 sur des réseaux à commutation de paquets.
  - Egalement sur des liaisons point-à-point, si elles ne sont pas fiable ou possèdent un délai inhérent (Exemple : liaison par satellite).
  - Apporte la fiabilité et le contrôle de flux sur une base point-à-point.
- **HDLC** (High-Level Data Link Control) **:**
  - Incompatible entre fournisseurs car chacun a sa propre mise en œuvre.
  - Prend en charge les configurations point-à-point et multipoints.
  - Dérivé du protocole SDLC (Synchronous Data Link Control) .
  - Protocole par défaut pour les interfaces série d'un routeur Cisco.
  - Extrêmement simplifié : Pas de fonctions de fenêtrage ni de contrôle de flux.
  - Champ d'adresse contenant uniquement des 1, avec un code propriétaire à 2 octets indiquant le type de verrouillage de trame du fournisseur.

Le protocole HDLC est recommandé sur une liaison reliant deux équipements utilisant IOS. Dans le cas contraire, il est recommandé d'utiliser le protocole PPP.

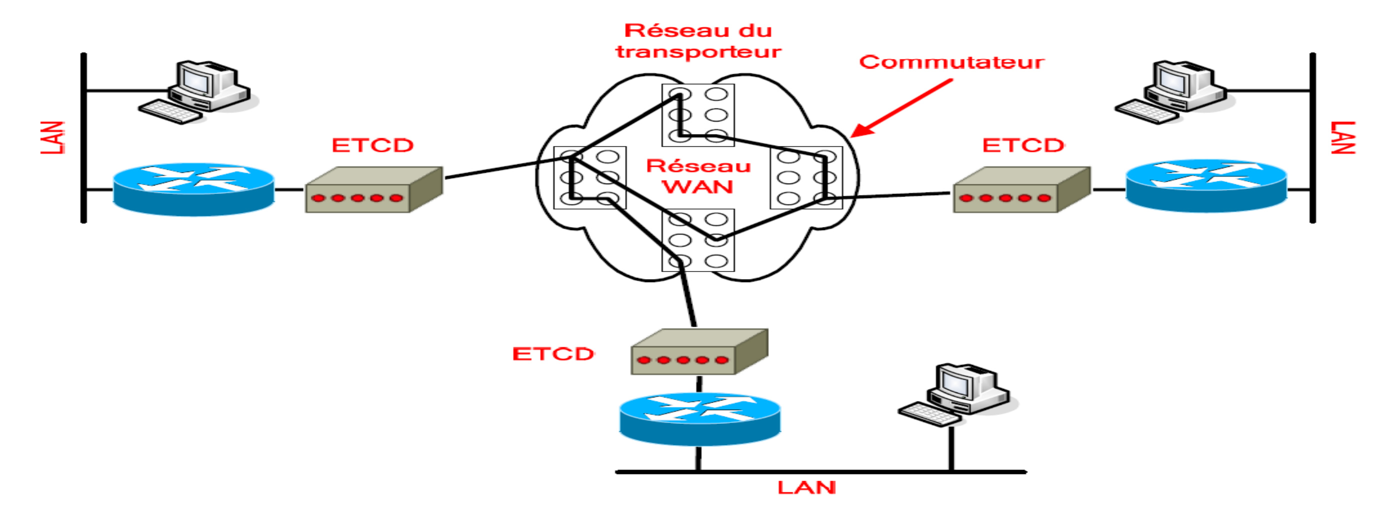
IV. Classement des différents types de liaison WAN



Les différents types de liaison WAN habituellement disponibles sont :

- **Liaisons dédiées** (aussi appelées liaisons spécialisées ou lignes louées) :
  - Fournissent un service continu.
  - Il s'agit d'un lien physique dédié qui va directement d'un port du routeur client à un port du routeur de l'opérateur, sans passer par un environnement commuté.
  - Il est nécessaire d'avoir un port par liaison client sur le routeur de l'opérateur.
  - Fournies par des liaisons série synchrone point-à-point.
  - Cette liaison point-à-point est utilisée pour Une liaison physique directe ou des liaisons virtuelles constituées de plusieurs liaisons physiques.
  - Conviennent aux grands volumes d'information et aux trafics constants.

- **Connexions commutées** :
  - A commutation de circuits : Commutation physique des centraux téléphoniques afin d'obtenir la liaison point-à-point.
  - A commutation de paquets/cellules : Commutation « logique » effectuée au niveau de la couche 2 du modèle OSI.



Autres types de liaisons WAN

- *xDSL (DSL pour Digital Subscriber Line et x pour désigner une famille de technologies)* pour un usage domestique. Offre une bande passante qui diminue en fonction de la distance par rapport à l'équipement de l'opérateur. Des vitesses maximales de 51,84 Mbits/s sont possibles à proximité d'un central téléphonique, mais des débits largement inférieurs sont plus courants (de quelques centaines de Kbits/s à plusieurs Mbits/s). D'un usage peu répandu, mais en augmentation rapide, son coût est modéré et en baisse. Le caractère x indique l'ensemble de la famille de technologies DSL, dont :
  - *HDSL* - Ligne numérique (DSL) à haut débit binaire
  - *SDSL* - Ligne numérique (DSL) à débit symétrique
  - *ADSL* - Ligne numérique à paire asymétrique (DSL asymétrique)
  - *VDSL* - Ligne numérique asymétrique (DSL) à très haut débit
  - *RADSL* - Ligne numérique (DSL) à débit adaptable

- *SONET (Synchronous Optical Network)* - Famille de technologies propre à la couche physique, offrant de très hauts débits et conçue pour la fibre optique. Elle peut aussi être utilisée avec des fils de cuivre. Elle offre une série de débits de données disponibles avec désignations spéciales. Elle est mise en œuvre à différents niveaux d'opérateur optique, de 51,84 Mbits/s (OC-1) à 9 952 Mbits/s (OC-192). Ces débits exceptionnels peuvent être atteints grâce au multiplexage en longueur d'onde, permettant aux lasers d'être réglés sur des couleurs (longueurs d'onde) légèrement différentes afin d'envoyer d'énormes quantités de données par voie optique. D'un usage répandu sur le backbone Internet, cette technologie reste d'un coût élevé (elle n'est pas utilisée pour raccorder les particuliers à Internet). SONET est la technologie utilisée en Amérique du Nord. L'équivalent européen s'appelle SDH (Synchronous Digital Hierarchy).

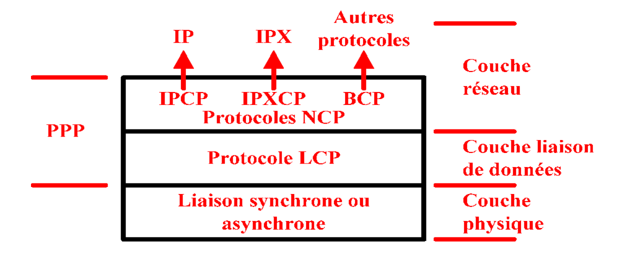
B. Protocole PPP

I. Etude du protocole

PPP (Point-to-Point Protocol) est le protocole de réseau WAN le plus répandu, successeur du protocole **SLIP** (Serial Line Internet Protocol), permettant :

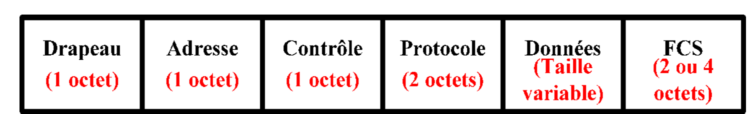
- Connexion entre routeurs ou entre un hôte et un routeur.
- Gestion des circuits synchrones et asynchrones.
- Contrôle de la configuration des liaisons.
- Possibilité d'attribution dynamique des adresses de couche 3.
- Multiplexage des protocoles réseau (Possibilité de faire passer plusieurs paquets de protocoles différents sur la même connexion).
- Configuration des liaisons et vérification de leur qualité.
- Détection des erreurs.
- Négociation d'options (Adresses de couche 3, Compression, etc.).

Le protocole **PPP** est composé de trois parties distinctes indispensables :



- **Un mode d'encapsulation** : La trame PPP est une trame générique HDLC (High-Level Data Link Control) modifiée.
- **Le protocole LCP** (Link Control Protocol) : Etablissement et contrôle d'une session.
- Trame LCP d'établissement de liaison.
- Trame LCP de fermeture de liaison.
- Trame LCP de maintenance de liaison.
- **Une famille de protocoles NCP** (Network Control Protocol) : Gestion des protocoles de couche 3.
  - **IPCP** (Internet Protocol Control Protocol).
  - **IPXCP** (Internetwork Packet eXchange Control Protocol).
  - **BCP** (Bridge Control Protocol).

Une trame **PPP** est de la forme :



Drapeau (1 octet)	Adresse (1 octet)	Contrôle (1 octet)	Protocole (2 octets)	Données (Taille variable)	FCS (2 ou 4 octets)

- **Drapeau :** Indicateur de début ou fin de trame (Valeur = 01111110).
- **Adresse :** Adresse de broadcast standard (Valeur = 11111111), car PPP n'attribue pas d'adresse d'hôte (Couche 2).
- **Contrôle :** Fourniture d'un service non orienté connexion (Valeur = 00000011).
- **Protocole :** Identification du protocole encapsulé (IP, IPX, etc.).
- **Données :** Contient soit la valeur zéro, soit des données (1500 octets maximum).
- **FCS :** Séquence de contrôle de trame pour une vérification des erreurs.

II. Etablissement d'une session

Les quatre phases d'une session PPP, pour l'établissement des communications sur une liaison point-à-point, sont :

- **Établissement de la liaison.**
- **Détermination de la qualité de la liaison.**
- **Configuration du ou des protocoles de couche réseau.**
- **Fermeture de la liaison.**

Ce sont les trames LCP qui se chargent du bon déroulement de ces quatre phases.
Phase 1 - Etablissement de la liaison :

- Le nœud d'origine envoie des trames LCP pour configurer et établir la liaison.
- Négociation des paramètres de configuration grâce au champ d'option des trames LCP (MTU, compression, authentification, etc.). Ces options peuvent donc être explicite (indiquées dans les trames LCP) ou implicites (Utilisation des valeurs par défaut).
- Fin de cette phase par l'émission et la réception d'une trame LCP d'accusé de réception de la configuration.

Phase 2 - Détermination de la qualité de la liaison :

- Cette phase est facultative.
- Vérification de la qualité suffisante pour activer les protocoles de couche 3.
- Une fois la liaison établie, le processus d'authentification est lancé, si nécessaire.

Phase 3 - Configuration du ou des protocoles de couche réseau :

- Émission de paquets NCP pour configurer les protocoles de couche 3 choisis.
- Configuration individuelle des protocoles de couche 3 grâce au protocole NCP approprié.
- Activation et fermeture à tout moment des protocoles de couche 3.
- Les paquets des protocoles de couche 3 sont émis une fois configuré par son NCP correspondant.

Phase 4 - Fermeture de la liaison :

- Fermeture par le biais de trames LCP ou de paquets NCP spécifiques (Si LCP ferme la liaison, il informe les protocoles de couche 3 par l'intermédiaire du NCP correspondant).
- Fermeture à cause d'un évènement extérieur (délai d'attente, perte de signaux, etc.).
- Fermeture en cas de demande d'un utilisateur.

On peut vérifier l'état des protocoles LCP et NCP grâce à la commande **show interfaces.**

III. Authentification

Le protocole PPP peut prendre en charge plusieurs modes d'authentification :

- Aucune authentification.
- Utilisation du protocole PAP (Password Authentication Protocol).
- Utilisation du protocole CHAP (Challenge Handshake Authentication Protocol).

Les caractéristiques du protocole PAP sont :

- **Échange en deux étapes** (après la demande d'authentification) :
- Envoie des informations d'authentification.
- Acceptation ou refus.
- **Méthode simple d'authentification** : Emission de la combinaison utilisateur/password de façon répétée jusqu'à :
- Confirmation de l'authentification.
- Interruption de la connexion.
- **PAP** n'est pas très efficace **:**
- Mots de passe envoyés en clair.
- Aucune protection (Lecture répétée des informations, attaques répétées par essais et erreurs).
- Le nœud s'authentifiant contrôle la fréquence et la durée des tentatives d'authentification.
- Pour le protocole PAP, on a le choix entre une authentification :
- **Unidirectionnelle** : Seul le client est authentifié sur le serveur de compte.
- **Bidirectionnelle** : Chaque hôte authentifie l'autre.

Celles du protocole CHAP sont :

- **Échange en trois étapes** (après la demande d'authentification) :
- Confirmation.
- Réponse.
- Acceptation ou refus.
- **Méthode d'authentification plus évoluée** :
- Vérification régulière de l'identité du nœud distant (A l'établissement puis à tout moment).
- Authentification dans les deux sens.
- Impossibilité de tenter une authentification sans avoir reçu une demande de confirmation.
- Authentification cryptée via l'algorithme MD5 lors du transit sur la liaison.
- **Efficacité contre le piratage** :

- Utilisation d'une valeur de confirmation variable, unique et imprévisible.
- Répétition des demandes de confirmation visant à limiter la durée d'exposition aux attaques.
- Chaque côté contrôle la fréquence et la durée des tentatives d'authentification.

IV. Configuration

Les commandes permettant de configurer tous les différents aspects du protocole PPP sont les suivantes :

- **username {nom} password {mot_de_passe} :**

- Mode de configuration globale.
- Paramètre nom : Nom d'hôte qu'on souhaite accepter.
- Paramètre mot_de_passe : Mot de passe à utiliser pour l'authentification. Celui-ci doit correspondre au mot de passe du mode privilégié crypté du routeur distant si on utilise CHAP. Ce mot de passe doit être le même sur les deux routeurs.
- Définir un compte d'utilisateur localement, afin de permettre l'authentification d'un hôte distant.

- **encapsulation PPP :**

- Mode de configuration d'interface.
- Spécifier le mode d'encapsulation pour l'interface courante.

- **ppp authentication {chap | chap pap | pap chap | pap} [callin] :**

- Mode de configuration d'interface.
- Définir la méthode d'authentification voulue. On a la possibilité de définir deux méthodes différentes. Dans ce cas, la première est utilisée, et en cas de refus ou de suggestion de la deuxième, la deuxième méthode sera utilisée.
- Le paramètre callin est utilisé pour différencier l'authentification unidirectionnelle de la bidirectionnelle.

- **ppp pap sent-username {nom} password {mot_de_passe} :**

- Mode de configuration d'interface.
- Indique les informations qui seront envoyées lors d'une demande d'authentification PAP. Les informations doivent correspondre au compte utilisateur définit sur le routeur distant.

- **ppp chap hostname {nom} :**

- Mode de configuration d'interface.
- Permettre l'authentification sur plusieurs routeurs en donnant toujours le même nom d'hôte.

- **ppp chap password {mot_de_passe} :**

- Mode de configuration d'interface.
- Idem que pour le hostname, mais pour le mot de passe. Ceci permet de limiter le nombre d'entrées utilisateur/password.

- **ppp quality {pourcentage} :**

- Mode de configuration d'interface.
- Permet de configurer le LQM (Link Quality Monitor) sur la liaison PPP courante. Si la qualité de la liaison tombe en dessous du pourcentage spécifié, le routeur coupera la liaison.

Pour tout problème concernant l'authentification et la négociation de liaison par rapport au protocole PPP, nous avons à notre disposition les commandes suivantes :

- **debug ppp authentication**
- **debug ppp negociation**

4.1. Procédure de configuration du protocole PAP

Nous allons d'abord étudier la configuration qu'il faut utiliser pour une authentification unidirectionnelle.



```
Lab_A (config-if)# encapsulation ppp
Lab_A (config-if)# ppp authentication pap
Lab_A (config-if)# ppp pap sent-username Lab_A  password password_pap
```

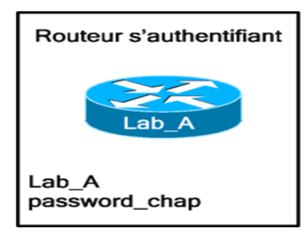
```
Lab_B (config)# username Lab_A  password password_pap
Lab_B (config-if)# encapsulation ppp
Lab_B (config-if)# ppp authentication pap
```

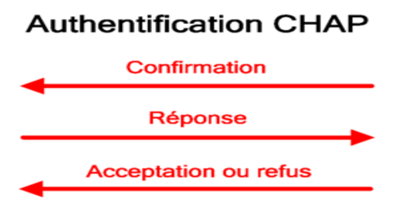
Pour une authentification bidirectionnelle, il suffit de procéder comme suit :

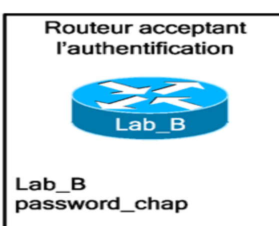
```
Lab_A (config)# username Lab_B  password password_pap
Lab_A (config-if)# encapsulation ppp
Lab_A (config-if)# ppp authentication pap
Lab_A (config-if)# ppp pap sent-username Lab_A password password_pap
Lab_B (config)# username Lab_A password  password_pap
Lab_B (config-if)# encapsulation ppp
Lab_B (config-if)# ppp authentication pap
Lab_B (config-if)# ppp pap sent-username Lab_B password password_pap
```

4.2. Procédure de configuration du protocole CHAP

Le schéma d'authentification ci-dessus représente l'authentification dans un seul sens, il va donc falloir répéter ce schéma dans les deux sens de l'authentification CHAP.







Pour cela, nous allons effectuer les tâches de configuration suivantes sur le routeur Lab_A :

```
Lab_A (config)# username Lab_B  password password_chap
Lab_A (config-if)# encapsulation ppp
Lab_A (config-if)# ppp authentication chap
```

Les commandes à utiliser sur le routeur Lab_B sont :

```
Lab_B (config)# username Lab_A password password_chap
Lab_B (config-if)# encapsulation ppp
Lab_B (config-if)# ppp authentication chap
```

C. Protocole Frame Relay

I. Introduction

Le relayage de trames (ou FR, pour l'anglais Frame Relay) est un protocole à commutation de paquets situé au niveau de la couche de liaison (niveau 2) du modèle OSI, utilisé pour les échanges intersites (WAN) il a été inventé par Eric Scace, ingénieur chez Sprint International.

Sur le plan historique, il peut être vu :

1. comme un successeur de X.25 : il a en effet remplacé ce protocole pour le raccordement des sites des entreprises aux infrastructures des opérateurs qui offrent des services RPV.
2. comme une étape vers l'ATM : il a souvent été présenté ainsi par les opérateurs « très » UIT (Union internationale des télécommunications), c'est-à-dire les opérateurs ayant « voulu » X.25 et l'ATM, comme France Télécom par exemple. Le Frame Relay est en effet issu d'une volonté américaine, en particulier de l'ANSI (American National Standards Institute), X.25 n'ayant jamais été très populaire aux États-Unis.
3. comme faisant partie du RNIS (ISDN) : c'est ainsi que l'UIT l'a considéré.

Sur le plan intérêt économique :

4. le Frame Relay est une technologie qui permet de remplacer les liaisons louées (coûteuses car dédiées à un seul client) par un "nuage" Frame Relay mutualisé entre de nombreux clients. Le fournisseur d'accès partant du principe qu'il y a peu de chances que tous ses clients aient besoin d'une bande passante maximale simultanément propose à ses clients un contrat indiquant un Excess Information rate (ou burst), c'est-à-dire le débit maximum accepté sur le réseau Frame Relay et un CIR (Committed Information Rate), c'est-à-dire un débit garanti minimum. Aux États-Unis, le relais de trames a ainsi pris une grosse part du marché des liaisons louées puisqu'en fin 2001 les entreprises utilisaient autant de portes relais de trames que de liaisons louées pour raccorder leurs sites
5. remplacement du X.25 : les entreprises ont effectivement migré leurs réseaux de X.25 vers le relais de trames pour les migrer depuis 2004 vers des offres de RPV IP

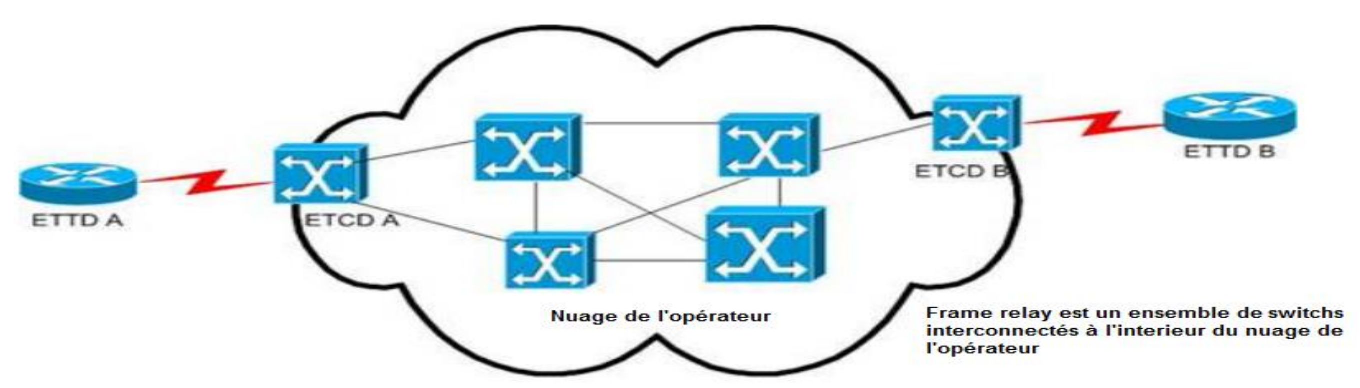
Sur le plan technique :

6. Les réseaux Frame Relay fournissent plus de fonctionnalités et de bénéfices que les connexions point-à-point
   - si nous devions interconnecter 10 routeurs entre eux par des connexions point à point dédiées, nous aurions besoin de 45 lignes louées (9+8+7+...+2+1=10*9/2)
   - avec Frame Relay, grâce à la notion de chemin virtuel, nous n'avons besoin que de 10 lignes.
7. Les réseaux Frame Relay sont des réseaux à accès multiples comme les protocoles des LAN
   - plusieurs périphériques peuvent être connectés au réseau
   - Il est impossible d'envoyer une trame à plusieurs périphériques en une seule fois, les réseaux Frame Relay sont NBMA (Non broadcast Multi access networks).
8. Les réseaux Frame Relay présentent les caractéristiques suivantes :
   - débit compris entre 56kb/s et 2 Mb/s, voir plus
   - comme les moyens de communication actuels sont de moins en moins responsables des erreurs sur les données, Frame Relay n'introduit que très peu de contrôle d'erreurs.
   - il ne possède ni fenêtrage, ni mécanisme de retransmission
   - il peut être utilisé à la fois dans un réseau public et dans un réseau privé

II. Technologie Frame relay

2.1. Equipements nécessaires au Frame relay

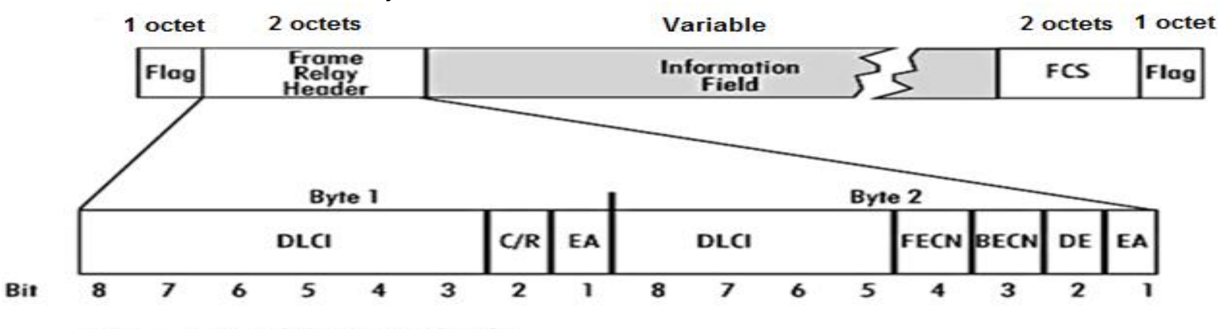
Les routeurs (considérés comme des DTE : *Data Terminal Equipment* ETTD en français) sont connectés à des Switchs Frame Relay (considérés comme des DCE : *Data Communications Equipment* ETCD en français) par des lignes spécialisées.
Ces liens entre routeurs et Switchs Frame Relay sont appelés des liens d'accès sur lesquels sont périodiquement transportés des messages définis par le protocole *Local Management Interface* (LMI)



- L'ETTD (Equipement Terminal de Traitement de Données) est un équipement (généralement un routeur) de terminaison de réseau placé chez le client du fournisseur FR.
- L'ETCD (Équipement Terminal de Circuit de Données) est un équipement fournissant des services d'horloge et de commutation placé chez le fournisseur d'accès.

2.2. Encapsulation Frame Relay

Le format des trames Frame Relay est le suivant :



- **Les champs DELIMITEUR (*Flag*) :** toutes les trames commencent et se terminent par un flag. Le fanion a pour motif 0x7E (01111110). Pour éviter de retrouver le pattern des flags n' importe où dans la trame, il a été mis en place la « Technique d'insertion de zéros à l'émission » et « la désinsertion de zéros à la réception ». Ceci permet d'être sûr qu'il n'y a pas de pattern 0x7E dans la séquence de bits à transmettre entre le flag du début et celui de la fin.

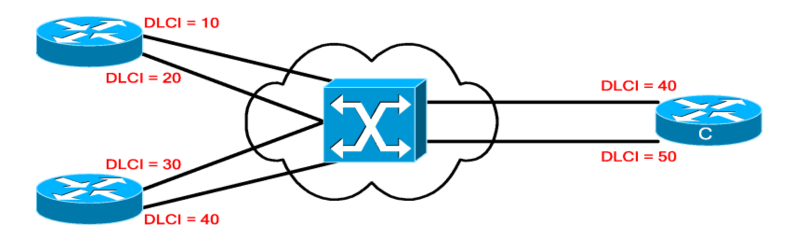
- **Le champ DLCI (Data Link Connexion Identifier) :** le Champ DLCI (Data Link Connexion Identifier) identifie le numéro de voie logique entre ETTD et ETCD de 1 à 1023. Le commutateur associe le numéro de voie logique à une destination pour créer ainsi un circuit virtuel avec un autre correspondant. A l'instar de ce que permet X25, plusieurs d'entre eux pouvant être multiplexés sur un même support, physique. De la même manière, le DLCI n'a qu'une signification locale utilisée par convention entre un ETTD et son ETCD de rattachement. Il peut y avoir plusieurs connexions virtuelles sur le même support physique.

- **Le champ C/R :** commande Réponse, ce bit n'est pas interprété par les nœuds du réseau mais peut éventuellement l'être par les systèmes utilisateurs situés à chaque extrémité.

- **Les bits « FECN » et « BECN »** : Le bit FECN est positionné à 1 par un réseau pour indiquer à l'ETTD recevant la trame qu'une congestion a été détectée de la source vers le destinataire. Le bit BECN indique au même ETTD qu'une congestion a été détectée dans l'autre sens. Ces bits peuvent être utilisés par les couches de niveau 3 pour contrôler le flux soit du récepteur, soit de l'émetteur.
- **Le bit « DE »** : Il est positionné à 1 par ETTD pour indiquer au commutateur que la trame à moins d'importance que les autres et peut être détruite si le réseau manque de ressource (CPU ou mémoire…), notamment dans le cas des congestions. Inversement, les commutateurs du réseau peuvent d'office positionner ce bit à « 1 » pour indiquer à la station qu'elle rengorge le réseau et que les trames suivantes risquent d'être détruites.
- **Le bit « EA »** : Il indique que l'adresse DLCI est étendue au-delà de 2 octets de base.
- **Le champ « DONNEES » :** Ce champ contient les données à transporter. La longueur maximum peut être négociée au moment de l'établissement de circuit virtuel. La taille par défaut est de 262 octets mais il est recommandé que le réseau puisse supporter des tailles de trames de 1600 octets.
- **Le champ « FCS »** : Ce champ est utilisé pour le contrôle d'erreur sur la trame. Il est basé sur le calcul d'un CRC16 et correspond au polynôme ($x^{16} + x^{12} + x^5 +1$). Le Frame Check Sequence effectue un contrôle sur tous les bits de la trame à l'exception des en-têtes et en-queues.

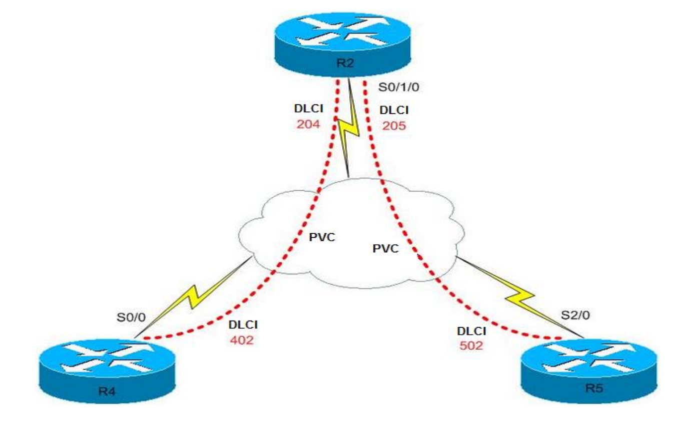
2.3. Les circuits virtuels

- Un circuit virtuel défini un chemin logique entre 2 extrémités (2 Frame Relay DTE) : Permet de créer une connexion point à point entre deux équipements à travers un WAN sans qu'il y ait réellement de circuit physique qui les relie.
- Les routeurs utilisent des data-link connection identifier (DLCI) comme adresses Frame Relay : Les DLCI permettent de désigner les circuits virtuels (VC) qui seront utilisés pour transmettre les données vers la destination.



  - Les identificateurs DLCI sont reconnus localement, ce qui implique qu'ils ne sont pas forcément uniques dans le nuage Frame Relay (Exception faite si on utilise l'extension LMI d'adressage global). Deux unités ETTD peuvent utiliser une valeur DLCI identique ou différente pour désigner le PVC les reliant.
  - L'espace d'adressage DLCI est limité à 10 bits. Une partie de la plage d'adresse (0 à 1023) est utilisable pour les adresses d'extrémité (Transport des données utilisateur de 16 à 1007), et le reste est réservé à des fins d'implémentation par le constructeur (Messages LMI, adresses de multicast, etc.).

- Il existe deux types de circuits virtuels : permanents (PVC) et commutés (SVC) :
  - Les PVC sont pré-configurées par l'opérateur lors de l'abonnement
  - Les SVC sont établis dynamiquement à l'initiative de l'usager.



2.4. Protocole Local Management Interface (LMI)

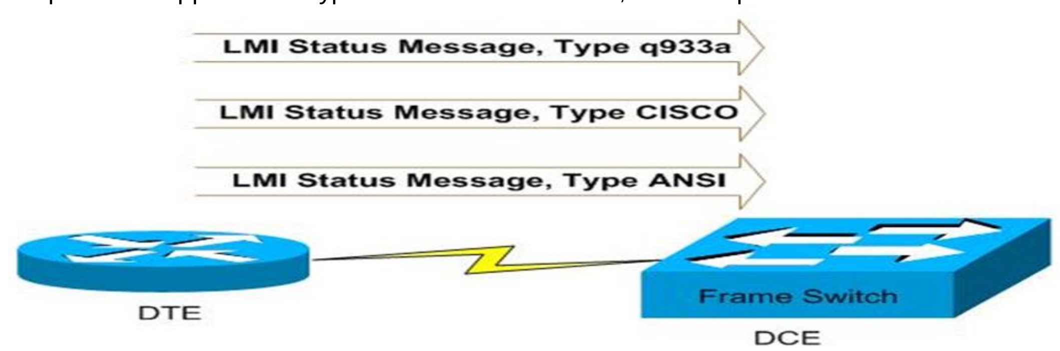
La mise en œuvre et le fonctionnement de la technologie Frame Relay repose essentiellement sur les interfaces LMI, dont les fonctions de base sont :

- Déterminer la fonctionnalité des PVC connus du routeur.
- Transmettre des messages de veille, pour éviter que le PVC ne se ferme pour cause d'inactivité.
- Indiquer au routeur les PVC disponibles.

Il existe des extensions LMI, qui sont optionnelles :

- **Messages d'état des circuits virtuels (Extension universelle)** : Signalisation périodique sur les PVC (Nouveaux, supprimés, leur intégrité, etc.).
- **Diffusion multicast (Extension facultative)** : Permet la diffusion des messages de protocole de routage et ARP, qui doivent être normalement transmis à plusieurs destinataires. Cela utilise les DLCI 1019 à 1022.
- **Adressage global (Extension facultative)** : Portée globale des DLCI au lieu d'être locale. Permet d'avoir un DLCI unique sur le réseau Frame Relay.
- **Contrôle de flux simple (Extension facultative) :** Contrôle de flux de type XON/XOFF, destiné aux unités dont les couches supérieures ne peuvent pas utiliser les bits de notification de congestion, mais nécessitant un niveau de contrôle de flux.

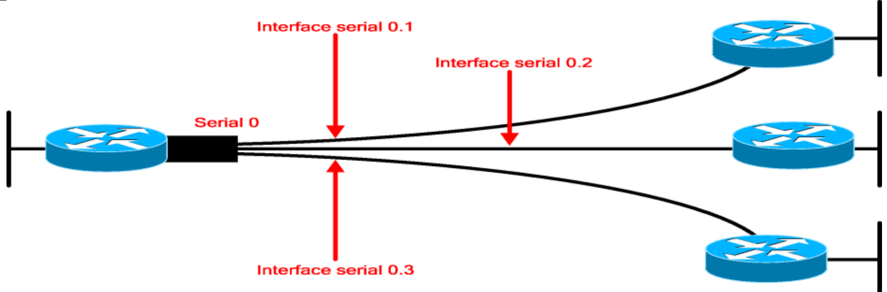
Le routeur peut faire appel à trois types d'interface LMI : ansi, cisco et q933a.



La portion exploitable de la plage d'adresse DLCI est définie par le type LMI utilisé :

- **ansi** : La plage de DLCI hôte va de 16 à 992.
- **cisco** : Les DLCI hôte vont de 16 à 1007.
- **q933a** : Même plage DLCI que la version **ansi.**

2.5. Les sous interfaces Frame Relay

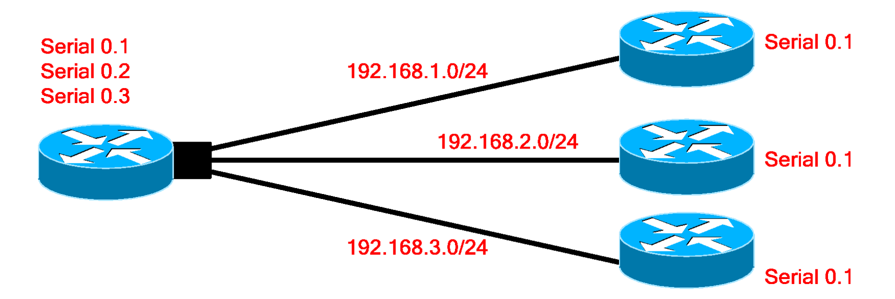


Les sous-interfaces sont des subdivisions logiques d'une interface physique et sont de deux types :

- Point-à-point.
- Multipoint.

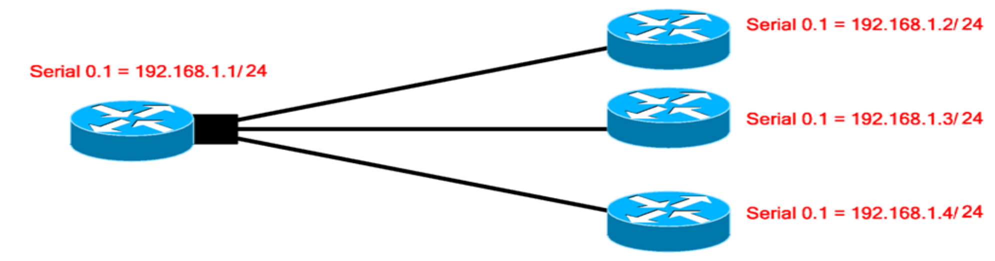
❖ Les caractéristiques des sous-interfaces point-à-point sont :

- Une sous-interface par PVC.
- Une attribution statique de DLCI par sous-interface.
- Chaque connexion point-à-point a son propre sous-réseau.
- Chaque interface possède un seul DLCI.
- Split horizon ne fonctionne pas comme on voudrait qu'il fonctionne dans le principe, car il ne connaît pas le principe de sous-interface, ce qui veut dire que les mises à jour de routage ne seront pas propagées vers les autres sous-interfaces.



❖ Les caractéristiques des sous-interfaces multipoints sont :

- Une seule sous-interface pour établir plusieurs PVC.
- Autant d'attributions statiques de DLCI qu'il y a de PVC (Destinataires).
- Toutes les interfaces font partie du même sous-réseau.
- Chaque interface possède son DLCI local.
- Split horizon fonctionne avec ce type de sous-interface.



III. Les commandes

Les commandes concernant Frame Relay sont les suivantes :

- **interface serial {numéro} :**
  - Mode de configuration globale.
  - Permet de passer dans le mode de configuration de l'interface souhaitée.
- **interface serial {numéro.sous-numéro} {multipoint | point-to-point} :**
  - Mode de configuration globale.
  - Permet de passer dans le mode de configuration de la sous-interface souhaitée.
  - Le paramètre multipoint ou point-to-point définit le type de sous-interface utilisée.
  - Il faut utiliser multipoint si on veut que le routeur envoie les broadcast et les mises à jour de routage qu'il reçoit.
- **encapsulation frame-relay [ietf] :**
  - Mode de configuration d'interface.
  - Précise l'encapsulation des trames pour l'interface courante.
  - Le paramètre cisco est la valeur par défaut, et est à utiliser si on est raccordée à un autre équipement Cisco.
  - Le paramètre ietf est utile pour se connecter à un dispositif non Cisco.
- **frame-relay interface-dlci {dlci} :**
  - Mode de configuration de sous-interface.
  - Affecte un DLCI pour la sous-interface courante.
- **frame-relay local-dlci {dlci} :**
  - Mode de configuration d'interface.
  - Permet d'affecter manuellement le DLCI pour l'interface courante (normalement attribué automatiquement par le LMI).
  - Il faut utiliser cette commande dans les environnements ne supportant pas les interfaces LMI.
- **frame-relay lmi-type {ansi | cisco | q933a} :**
  - Mode de configuration d'interface.
  - La valeur cisco est par défaut.
  - Cette commande est à utiliser uniquement pour une version d'IOS ancienne car, avec les versions 11.2 et ultérieure, le type de LMI est détecté automatiquement.
- **bandwidth {bp}** :
  - Mode de configuration d'interface.
  - Permet de spécifier la bande passante de la liaison sur un ETTD, à titre d'information (Pour un protocole de routage).

- **frame-relay inverse-arp {protocole} {dlci} :**
  - Mode de configuration d'interface.
  - Active la résolution d'adresse inverse pour le protocole de couche 3 indiqué en paramètre.
  - Cette résolution est active par défaut.
- **frame-relay map {protocole} {adresse} {dlci} [broadcast] :**
  - Mode de configuration d'interface.
  - Permet de mapper localement une adresse de couche 3 distante avec le DLCI local par lequel passer pour atteindre cette destination.
- **frame-relay intf-type {dte | dce | nni} :**
  - Mode de configuration d'interface.
  - Permet d'expliciter le type d'interface Frame Relay locale.
  - La valeur par défaut est **dte.**
  - **dce** est à utiliser pour l'interface du commutateur Frame Relay reliée au DTE (ETTD), et **nni** est pour les interfaces reliant les commutateurs Frame Relay.
- **frame-relay switching :**
  - Mode de configuration globale. Permet d'activer la commutation de PVC sur une unité ETCD (Commutateur Frame Relay).
  - Active l'interface LMI.
- **frame-relay route {dlci_src} interface {type} {numéro} {dlci_dest} :**
  - Mode de configuration d'interface.
  - Permet de créer une entrée dans la table de commutation Frame Relay.
  - Il faut indiquer le DLCI source, l'interface locale de sortie et celui de la destination.
  - Cette commande est à utiliser sur un commutateur Frame Relay uniquement.

IOS met à notre disposition des commandes de visualisation d'état et de débogage afin de pouvoir vérifier le bon fonctionnement des points spécifiques à Frame Relay, ainsi que d'identifier les problèmes éventuels :

- **show interfaces serial {numéro} :** Affichage des informations sur les DLCI utilisés et sur l'indicateur de connexion de liaison de données LMI utilisé.
- **show frame-relay pvc :** Affichage de l'état de chaque connexion configurée ainsi que les statistiques sur le trafic. Cette commande permet aussi de savoir le nombre de paquets BECN et FECN reçus par le routeur.
- **show frame-relay map :** Affichage de l'adresse de couche 3 ainsi que le DLCI associé à chaque destination distante connectée au routeur local.
- **show frame-relay lmi** : Affichage des statistiques sur le trafic LMI.
- **show frame-relay route** : Affichage des routes Frame Relay configurées avec leur statut.
- **show frame-relay traffic :** Affichage des statistiques Frame Relay globales (Requêtes ARP, etc.).
- **debug frame-relay events** : Affichage des réponses aux requêtes ARP.
- **debug frame-relay lmi** : Affichage des échanges de paquets LMI entre le routeur et le commutateur.
- **debug frame-relay packet** : Analyse des paquets Frame Relay envoyés.

IV. Configuration

La procédure de configuration d'une interface (DTE) en Frame Relay passe par les étapes suivantes :

- Passer dans le mode de configuration de l'interface voulue (**Commande interface serial {numéro}**).
- Définir une adresse de couche 3 (**Commande ip address {IP} {SM}**).
- Définir le type d'encapsulation (**Commande encapsulation frame-relay**).
- Définir le DLCI local en cas de non support de l'interface LMI (**Commande frame-relay local-dlci {dlci}**).
- Définir optionnellement la bande passante de la liaison (**Commande bandwidth {bp}**).
- Activer l'interface (**Commande no shutdown**).

Cette même procédure change un peu lorsqu'il s'agit de sous-interfaces :

- Passer dans le mode de configuration de l'interface voulue.
- Enlever toute adresse de couche 3 (**Commande no ip address**).
- Définir le type d'encapsulation.
- Passer dans le mode de configuration de la sous-interface voulue (**Commande interface serial {if.subif} {point-to-point | multipoint}**).
- Définir une adresse de couche 3.

- Définir le ou les DLCI locaux, car le LMI ne supporte pas les sous-interfaces (**Commande frame-relay interface-dlci {dlci}**).
- Définir optionnellement la bande passante de la liaison.
- Activer la sous-interface.

Il est possible de simuler un commutateur Frame Relay à l'aide d'un routeur. Les interfaces utilisées sont alors obligatoirement de type DCE. Pour ce faire, il faut utiliser une configuration distincte pour chaque interface :

- Activer la commutation Frame Relay sur le routeur (**Commande frame-relay switching**).
- Passer dans le mode de configuration de chaque interface utilisée.
- Enlever toute adresse de couche 3.
- Définir le type d'encapsulation.
- Définir la vitesse de fonctionnement de la liaison (**Commande clock rate {valeur}**).
- Définir le type d'interface Frame Relay.
- Définir une route pour chaque destinations accessibles depuis la source raccordée sur l'interface courante (**Commande frame-relay route {dlci_src} interface serial {numéro} {dlci_dest}**).
- Activer l'interface.

Configuration par défaut d'une interface série

Par défaut une interface série est sur un type d'encapsulation **HDLC**.
Afin de faire du frame-relay, on est obligé de spécifier le type d'encapsulation: encapsulation frame-relay.
Une fois ceci fait la configuration par défaut est la suivante :

- LMI : autoconfiguration (via essai de tous les types) (Toujours sur une interface physique)
- Encapsulation : cisco
- PVC DLCI appris automatiquement au moyen des messages LMI
- Inverse ARP : utilisé par défaut et se met automatiquement en marche lorsqu'un VC est déclaré "up"

V. Mappage DLCI/IP

5.1. Définition :

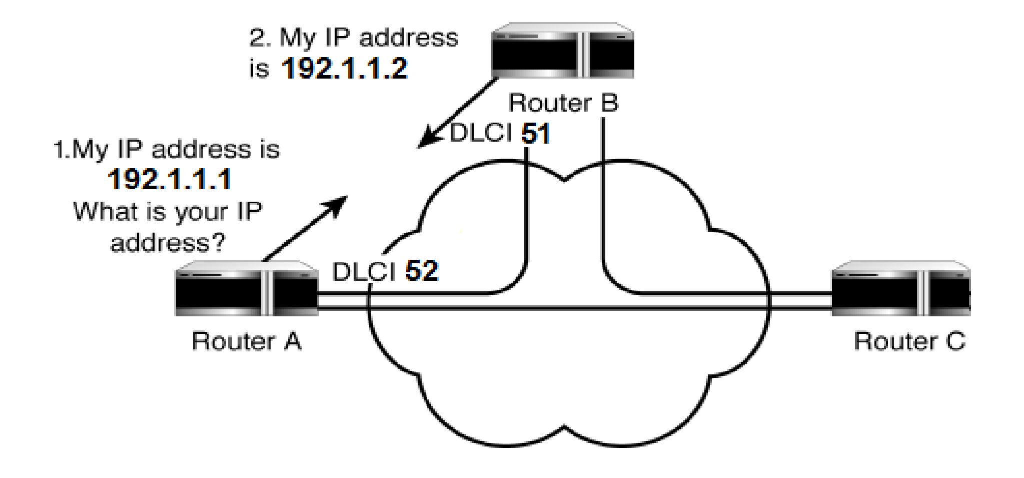
L'information qui permet de lier une adresse de niveau 3 à une adresse de niveau 2 s'appelle mappage. Cette information est nécessaire sur les réseaux de type multi-accès.

Afin de savoir comment se fait ce mappage les commandes suivantes sont très intéressantes :

show frame-relay pvc
show frame-relay map

5.2. Inverse ARP

Comment se fait le mappage dont on vient de parler ?
Celui-ci se fait en utilisant l'Inverse ARP. Contrairement à IP ARP, qui utilise une requête au moment où nous avons besoin de faire la correspondance IP/MAC, ici Frame-Relay "annonce" son IP une fois qu'un VC est déclaré "UP" ; ce qui permet d'associer un DLCI connu à une adresse IP.



5.3. Mappage statique DLCI/IP

Généralement, on utilisera l'Inverse ARP, néanmoins, on peut utiliser un mappage statique. Ceci se fait de la manière suivante :

```
R(config)# interface serial0/0
R(config-if)# no frame-relay inverse-arp
R(config-if)# frame-relay map ip 199.1.1.2 52 broadcast
R(config-if)# frame-relay map ip 199.1.1.3 53 broadcast
```

5.4. Création d'une sous-interface point à point

La création d'une sous-interface point à point (1 VC par sous-interface) se fait de la manière suivante :

```
R(config)#interface serial0/0/0
R(config-if)#encapsulation frame-relay
R(config-if)#interface serial 0/0/0.1 point-to-point
R(config-subif)#ip address 140.1.1.1 255.255.255.0
R(config-subif)#frame-relay interface-dlci 52
```

- Ici 'Inverse ARP' est activé et l'affectation du DLCI à la sous-interface est réalisée au moyen de frame-relay interface-dlci.
- L'avantage est de distinguer fortement une sous-interface avec une adresse IP différente par sous-interface.
- L'inconvénient => Plus de subnetting.

On pourrait configurer cela aussi de la manière suivante :

```
R(config-if)#interface serial 0/0/0.1 point-to-point
R(config-subif)#ip address 140.1.1.1 255.255.255.0
R(config-subif)#frame-relay map 140.1.1.2 52 broadcast
```

- En revanche configurer ainsi, 'Inverse ARP' est désactivé.

5.5. Création d'une sous-interface multipoint

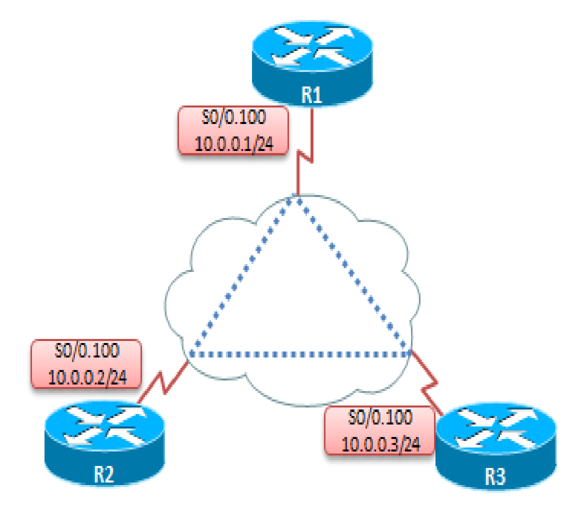
La configuration en mode multipoint (plusieurs VC par sous-interface) se fait de la manière suivante :

```
R(config)#interface serial0/0/0
R(config-if)#encapsulation frame-relay
R(config-if)#interface serial 0/0/0.1 multipoint
R(config-subif)#ip address 140.1.1.1  255.255.255.0
R(config-subif)#frame-relay interface-dlci 502
R(config-subif)#frame-relay interface-dlci 503
```

- Nécessite de mapper TOUS les DLCI avec les IP de leur correspondant sur une même interface.

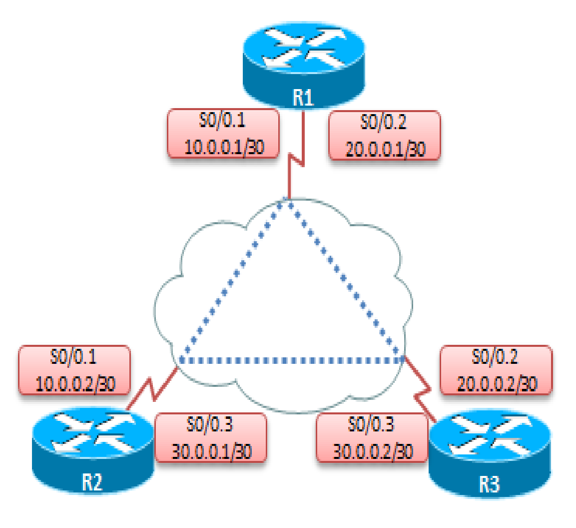
VI. Les différentes topologies frame-relay

6.1. Maillage complet (sous-réseau unique)



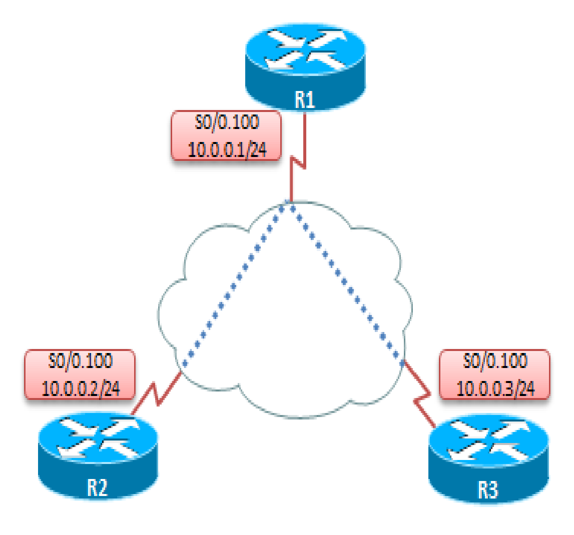
- Utilise une interface multipoint et un seul sous-réseau pour connecter chaque voisin.
- Configuration plus petite.
- Economiser de l'espace d'adresses IP.
- Repose sur ARP inversée pour les mappages.
- Si un PVC échoue, la communication entre les deux routeurs est perdue.

6.2. Maillage complet (sous-réseaux multiples)



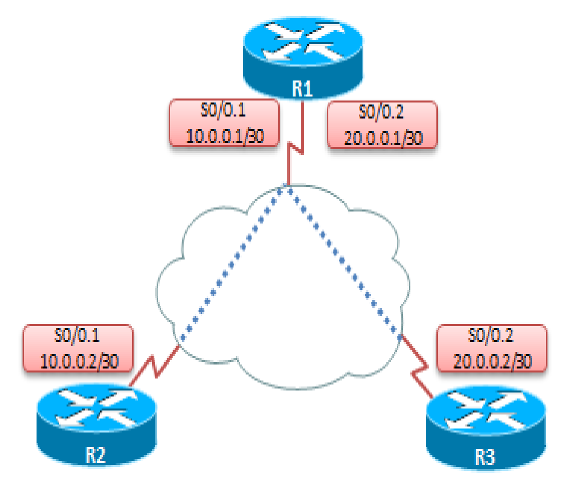
- Utilise les sous-interfaces Point-à-Point avec différents sous-réseaux pour connecter chaque voisin.
- Les exigences de la cartographie de sous-réseau sont simplifiées.
- Les protocoles de routage peuvent facilement fournir une redondance.

6.3. Hub-Spoke (sous-réseau unique)



- Principalement utilisé dans les laboratoires en raison de la complexité et les défis de cartographie, de broadcast et de décrémentation du TTL (parlé à rayons).
- Hub ne relaiera pas les broadcast d'un rayon à l'autre : les broadcats ne sont pas envoyés au-delà du routeur concentrateur.
- Hub ne relaiera pas l'ARP inversée donc les mappages doivent être fournis statiquement rayon à rayon.

6.4. Hub-Spoke (sous-réseaux multiples)



- R1 est le moyeu « Hub » semblable à un switch Ethernet
- R2 et R3 sont les rayons « Spokes »
- La configuration la plus typique.
- Utilise les sous-interfaces Point-à-Point avec différents sous-réseaux pour connecter les rayons au moyeu.
- Utilise les protocoles de routage pour acheminer entre les branches.

D. Services d'adressage IP

I. IPv6 : Internet Protocol version 6

1.1. Introduction

a. Généralités:
- Protocole de niveau 3 (couche Réseau)
- Successeur du protocole IPv4
- Protocole standard défini dans la RFC 2460

b. Types de communications IPv6:
- Unicast (de un à un)
- Multicast (de un à plusieurs)
- Anycast (de un au plus proche)

Remarque : Il n'y a plus de broadcast en IPv6 !!!

c. Points forts (par rapport à IPv4):
- Nombre d'adresses plus important ($3{,}4\times10^{38}$ adresses).
- Distribution des adresses en fonction des besoins et de la localisation géographique.
- Implémentation native du multicast (optionnel en IPv4) et de la sécurité (IPsec).
- Support accru pour la mobilité (roaming).
- En tête de protocole simplifié et mieux structuré.

d. En-tête IPv6 de base

Version	Traffic Class	Flow Label	Payload Length	Next Header	Hop Limit
Source IPv6 (128bits)					
Destination IPv6 (128bits)					

- Version : version du protocole (4 bits).
- Traffic Class : gestion de qualité de service (8 bits).
- Flow Label : marquage de flux pour traitement différencié dans le réseau (20 bits).
- Payload Length : taille du contenu en octets (16 bits).
- Next Header : identification de l'entête suivant (8 bits).
- Hop Limit : durée de vie du paquet, décrémenté d'une unité à chaque passage par un routeur. Le paquet est détruit si la valeur tombe à 0 (8 bits).

e. Méthodes d'attribution d'adresses
- Configuration statique
- Attribution par Statefull DHCP (DHCP traditionnel, fourni la configuration IPv6 complète de l'interface).
- Attribution par Stateless DHCP (Auto-configuration de l'interface selon le préfixe annoncé par le routeur. Seules les options sont fournies par le serveur DHCP).

1.2. Adresses IPv6

a. Principe
- Adresses codées sur 128 bits, divisées en 8 groupes de 4 caractères hexadécimaux séparés par « : ».
- L'identifiant réseau de l'adresse est nommé préfixe. La longueur du préfixe, sous la forme de /x, indique le nombre de bits dans l'identifiant réseau de l'adresse.
- Exemples :
  2001 : 0AB8 : 3409 : C0AB : 0001 : AEFF : FE00 : C801 /64 (exemple d'adresse globale)
  FE80 : 0000 : 0000 : 0000 : 021C : 2BFF : FE49 : ABCD (exemple d'adresse link-local)

b. Ecriture simplifiée des adresses IPv6
- Règle n°1 : Les groupes complets de 0 consécutifs peuvent être remplacés par « :: », une seule fois dans l'adresse.
- Règle n°2 : Les 0 non significatifs ne doivent pas être écrits.

- Exemple :

Adresse complète : 2001 : ABCD : 0000 : 0000 : 0ADE : 0000 : 0123 : C891
Règle n°1 : 2001 : ABCD : : 0ADE : 0000 : 0123 : C891
Règle n°2 : 2001 : ABCD : : ADE : 0 : 123 : C891

c. Adresses Globales Unicast

Adresses équivalentes aux adresses publiques IPv4, routables aussi bien dans un réseau privé que publique. La plage d'adresses 2000::/3 est réservée par l'IANA pour l'adressage publique (toutes les adresses commençant par les valeurs 2 et 3).

Format standard:

2001 : 0AD8 : 1234 :	0205 :	0000 : 0000 : 0000 : 0001
Préfixe global 48bits	Subnet ID 16 bits	Identifiant hôte 64 bits

Une société se voit attribuer le préfixe 2001 : 0AD8 : 1234 :: /48, si elle respecte le principe d'identifiant hôte de 64 bits, il reste 16 bits pour les découpes de sous-réseaux.

Remarque :
Le subnetting IPv6 respecte la même logique qu'en IPv4. Les adresses d'un même réseau ont le même identifiant réseau (appelé préfixe). La longueur du préfixe donnée en /x défini le nombre de bits de l'identifiant réseau.

d. Adresses « Unique Local » Unicast

Adresses équivalentes aux adresses privées IPv4, routables uniquement au sein d'un réseau privé.
La logique de subnetting correspond aux adresses globales, mais le préfixe « unique local » n'est pas géré globalement.
Les adresses « unique local » font partie de la plage FD00 :: /8 (toute adresse qui commence par FD).

Format standard:

FD	AB : 0102 : AACE :	0205 :	0000 : 0000 : 0000 : 0001
Unique Local 8bits	Global ID (pseudo aléatoire) 40bits	Subnet ID 16 bits	Identifiant hôte 64 bits

Le principe de subnetting des adresses « unique local » suit la même logique que les adresses globales. Le Global-ID est à choisir arbitrairement pour l'ensemble du réseau privé.

e. Adresses « Link-local »

Adresses ne fonctionnant qu'au sein du réseau local (au sens strict du terme, à savoir les machines dans le même subnet, dans le même domaine de diffusion, dans le même vlan…), ces adresses ne sont pas routables. Elles sont utilisées par les machines pour certains protocoles (protocole de routage, Neighbor Discovery, …).

Format:



Une interface pour laquelle on active IPv6 se génère automatiquement une adresse link-local, soit en générant les 64bits hôtes aléatoirement, soit en utilisant la méthode EUI-64 (voir ci-dessous).

Méthode EUI-64 « Extended Unique Identifier-64bits »
Méthode de génération d'un identifiant de 64 bits basé sur l'adresse MAC d'une interface.

Adresse MAC de base :	0001 : ACE1 : 000C 48bits de l'adresse MAC
Ajout de 16 bits (FF:FE) :	0001 : ACFF : FEE1 : 000C 64bits
Inversion du 7e bit :	0201 : ACFF : FEE1 : 000C EUI-64 terminé
	0201 en Binaire : 0000 0010 0000 0001

f. Adresses Multicast

Contrairement aux autres types, les adresses multicast ne sont pas attribuées à des interfaces, mais représentent un groupe d'interfaces cibles, dans un réseau local ou en dehors selon la portée de l'adresse.

La plage d'adresse FF00 :: /8 est réservée au multicast.

Adresses multicast particulières:

FF02 :: /16	Adresses multicast de portée locale
FF02 :: 1	Toutes les machines du réseau local (remplaçant du broadcast). Toute interface fonctionnant en IPv6 rejoint ce groupe.
FF02 :: 2	Tous les routeurs du réseau local.
FF02 :: 5	Tous les routeurs OSPFv3 du réseau local
FF02 :: 6	Tous les routeurs OSPFv3 DR/BDR du réseau local
FF02 :: 9	Tous les routeurs RIPng du réseau local
FF02 :: A	Tous les routeurs EIGRP du réseau local
FF02 :: 1 : FF00 :: / 104	« Sollicited Node multicast address » Adresse multicast dérivée d'une adresse configurée sur l'interface concernée

Remarque :
Une trame Ethernet qui véhicule un paquet IPv6 multicast aura généralement une adresse MAC destination multicast IPv6 sous la forme 3333.xxxx.xxxx (adresse MAC IPv6).

g. Adresses particulières

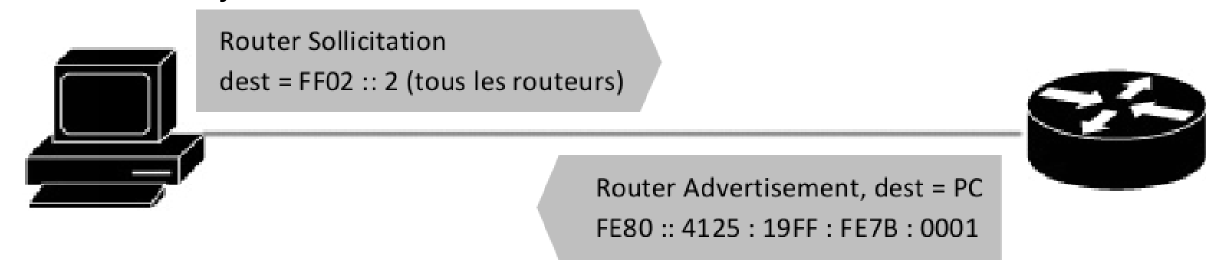
:: / 128	Adresse IPv6 indéterminée, utilisée par une machine pour remplir une information d'adressage quand elle n'en dispose pas encore (ex : requête DHCP).
:: 1 /128	Adresse loopback IPv6 (équivalent de 127.0.0.1 en IPv4)
:: / 0	Toute la plage d'adresses IPv6, utilisé pour la configuration d'une route par défaut, par exemple.

1.3. IPv6 Neighbor Discovery Protocol

Protocol servant principalement à la résolution des adresses physiques en fonction d'une adresse IPv6 pour les tâches suivantes :

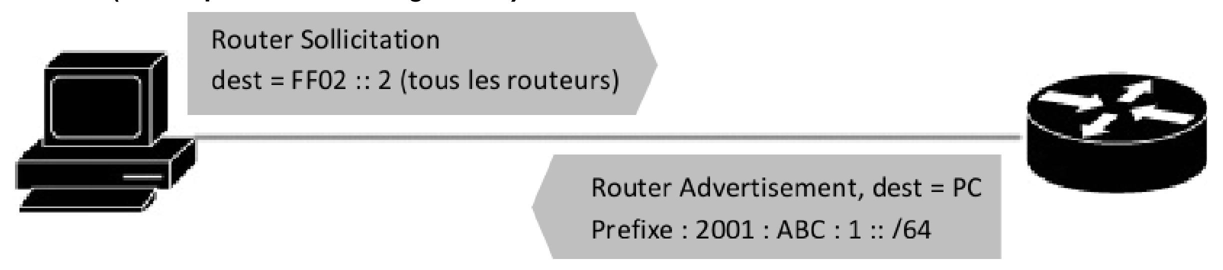
- Router Discovery : Découverte des routeurs présents dans le même réseau local.
- SLAAC : State Less Address Auto Configuration, messages du protocole NDP pour l'obtention du préfixe et de sa longueur auprès du routeur.
- Neighbor Discovery : Obtention d'une adresse MAC en fonction d'une adresse IPv6 (équivalent ARP).
- Duplicate Address Detection : Détection de duplication d'adresse dans le réseau local.

a. Router Discovery



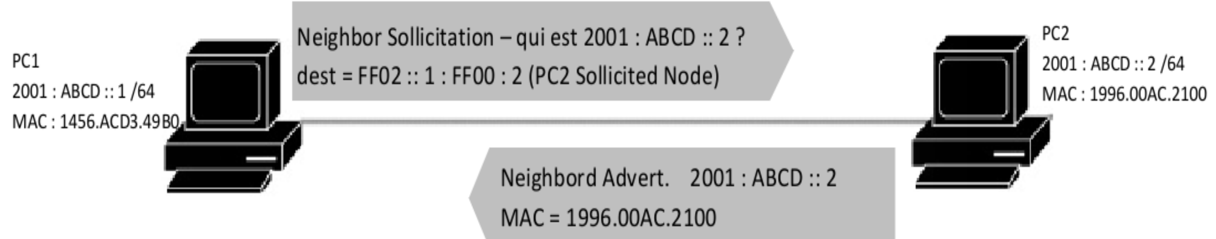
- ➢ PC émet un message NDP de type Router Sollicitation destiné à tous les routeurs (FF02 :: 2).
- ➢ Le router répond par un message Router Advertisement destiné au PC et contenant entre-autre son adresse link-local.

b. SLAAC (Utilisé pour l'auto-configuration)



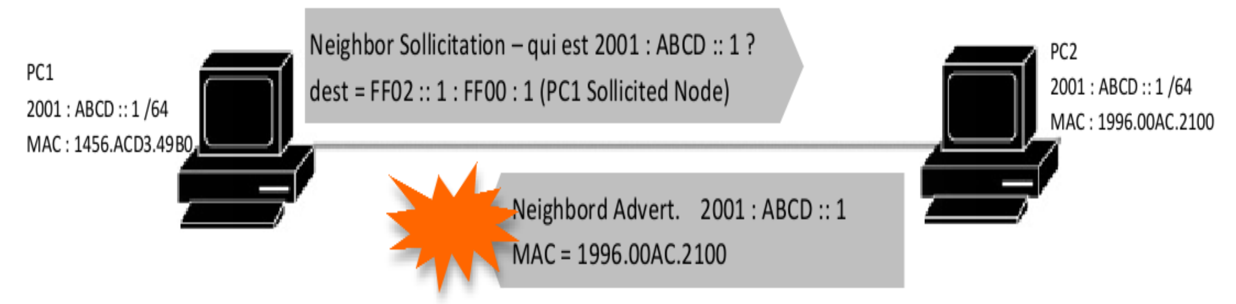
- PC émet un message NDP de type Router Sollicitation destiné à tous les routeurs (FF02 :: 2).
- Le router répond par un message Router Advertisement auquel il joint les informations relatives au préfixe et à sa longueur à utiliser sur le réseau.
- Le PC peut alors s'auto-configurer une adresse IPv6 en combinant le préfixe fourni et un identifiant hôte généré en EUI-64 ou aléatoirement.

c. Neighbor Sollicitation



- PC1 émet une message Neighbor Sollicitation destiné à l'adresse multicast « Sollicited Node », dérivée de l'adresse unicast recherchée (FF02 :: 1 : FFXX : XXXX , ou les X représentent la valeur des 24 derniers bits de l'adresse unicast).
- PC2 répond par un message de type Neighbor Advertisement en fournissant l'adresse MAC correspondant à son adresse unicast.

d. Duplicate Address Detection (DAD)



- PC1 émet un message Neighbor Sollicitation pour sa propre adresse.
- PC2 répond par un message de type Neighbor Advertisement en fournissant son adresse MAC pour la même adresse unicast.
- PC1 détecte alors que l'adresse est déjà en cours d'utilisation, vu qu'une autre machine que lui répond à la sollicitation.

1.4. Implémentation d'IPv6

a. Activation d'IPv6 sur une interface spécifique

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#ipv6 enable
R1(config-if)#no shutdown
```

Autorise la configuration d'adresses IPv6 sur l'interface concernée, et provoque la génération d'une adresse link-local.

```
R1#show ipv6 interface fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::C200:1FF:FEE7:0
  No Virtual link-local address(es):
  No global unicast address is configured
  Joined group address(es):
    FF02::1                 Groupe multicast « Tous les hôtes>
    FF02::1:FFE7:0          Groupe multicast « Sollicited node »
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
R1#
```

b. Activation du routage IPv6

```
R1(config)#ipv6 unicast-routing
```

Active les fonctionnalités de routage unicast IPv6, les interfaces actives en IPv6 rejoindront également le groupe multicast FF02 ::2 (tous les routeurs du réseau). Sans cette commande le routeur se comporte comme un simple hôte IPv6.

```
R1#show ipv6 interface fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::C200:1FF:FEE7:0
  No Virtual link-local address(es):
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2 ———————— Groupe multicast « Tous les routeurs »
    FF02::1:FFE7:0

  <suite de l'affichage omis par souci de brièveté>
```

c. Configuration d'une adresse unicast IPv6 manuelle (hors link-local ou anycast)

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#ipv6 address 2001:ABCD::1/64
```

Configure statiquement une adresse unicast. Ici les 128 bits de l'adresse sont définis.

```
R1#show ipv6 interface fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::C200:1FF:FEE7:0
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:ABCD::1, subnet is 2001:ABCD::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1 ———————— Groupe multicast « Sollicited Node »
                            correspondant à l'adresse unicast globale
    FF02::1:FFE7:0

  <suite de l'affichage omis par souci de brièveté>
```

d. Configuration d'une adresse unicast IPv6 EUI-64 (hors link-local ou anycast)

```
R2(config)#interface fastEthernet 0/0
R2(config-if)#ipv6 address 2001:ABCD::/64 eui-64
```

Configure l'adresse unicast globale selon la méthode EUI-64, 2001:ABCD::, suivi de l'identifiant EUI-64 dérivé de l'adresse MAC de l'interface.

```
R2#show interface fastEthernet 0/0 | include bia
  Hardware is Gt96k FE, address is c001.01e7.0000 (bia c001.01e7.0000)
R2#
R2#show ipv6 interface fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::C201:1FF:FEE7:0
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:ABCD::C201:1FF:FEE7:0, subnet is 2001:ABCD::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FFE7:0

  <suite de l'affichage omis par souci de brièveté>
```

e. Affichage de la table des voisins IPv6 («équivalent table ARP en IPv4)

```
R1#show ipv6 neighbors
IPv6 Address                              Age Link-layer Addr State
Interface
FE80::C201:1FF:FEE7:0                       1 c001.01e7.0000  STALE Fa0/0
2001:ABCD::C201:1FF:FEE7:0                  1 c001.01e7.0000  STALE Fa0/0

R1#
```

f. Configuration d'une adresse link-local

```
R2(config)#interface fastEthernet 0/0
R2(config-if)#ipv6 address FE80::2 link-local
```

Configure statiquement l'adresse link-local de l'interface.

```
R2#show ipv6 interface fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::2
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:ABCD::2, subnet is 2001:ABCD::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:2

  <suite de l'affichage omis par souci de brièveté>
```

Lorsque l'adresse link-local est configurée manuellement, elle modifie la valeur de l'EUI-64 également, modifiant ainsi l'adresse globale de l'interface si celle-ci utilise le format eui-64.

g. Affichage sommaire des interfaces IPv6

```
R1#show ipv6 interface brief
FastEthernet0/0            [up/up]
    FE80::C200:1FF:FEE7:0
    2001:ABCD::1
FastEthernet0/1            [administratively down/down]
R1#
```

Configure statiquement l'adresse link-local de l'interface.

h. Configuration d'une route statique IPv6

```
R1(config)#ipv6 route 2001:1234:1234:1234::/64 2001:ABCD::2
```

Configure une route statique vers le subnet 2001:1234:1234:1234 ::/64 utilisant 2001 :ABCD ::2 comme next-hop.

```
R1#show ipv6 route
IPv6 Routing Table - 4 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S   2001:1234:1234:1234::/64 [1/0]
     via 2001:ABCD::2
C   2001:ABCD::/64 [0/0]
     via ::, FastEthernet0/0
L   2001:ABCD::1/128 [0/0]
     via ::, FastEthernet0/0
L   FF00::/8 [0/0]
     via ::, Null0
R1#
```

i. Configuration d'une route statique IPv6 en utilisant l'adresse link-local du next-hop

```
R1(config)#ipv6 route 2001::/64 fastEthernet 0/0 FE80::2

R1#show ipv6 route
IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S   2001::/64 [1/0]
     via FE80::2, FastEthernet0/0
S   2001:1234:1234:1234::/64 [1/0]
     via 2001:ABCD::2
C   2001:ABCD::/64 [0/0]
     via ::, FastEthernet0/0
L   2001:ABCD::1/128 [0/0]
     via ::, FastEthernet0/0
L   FF00::/8 [0/0]
     via ::, Null0
R1#
```

II. NAT et PAT

1. Adressage privé et public

La très forte croissance et popularité d'Internet dans le début des années 90 ont mené très rapidement à la saturation des adresses pouvant être fournies par le protocole IP version 4. C'est entre autres pourquoi le système d'adressage privé a été élaboré, de manière à ralentir l'inévitable, à savoir l'épuisement de toutes les adresses IPv4.
Les plages d'adresses privées définies par la RFC 1918 sont les suivantes :

Classe d'adresses	Plage d'adresses privées	CIDR
A	De 10.0.0.0 à 10.255.255.255	10.0.0.0/8
B	De 172.16.0.0 à 172.31.255.255	172.16.0.0/12
C	De 192.168.0.0 à 192.168.255.255	192.168.0.0/16

- Ces plages d'adresses privées utilisées conjointement à la translation d'adresses, permettent à plusieurs réseaux d'utiliser les mêmes adresses. La translation d'adresse prend alors tout son intérêt en translatant, ou remplaçant, les adresses privées par une ou plusieurs adresses publiques afin de transiter sur Internet.
- Ceci crée donc plusieurs « cellules » d'adresses privées pouvant être identiques pour différents réseaux, sachant que chaque cellule ne serait accessible depuis Internet que par la ou les adresses publiques attribuées à chaque entreprise.
- Les adresses privées étant réservée à un usage interne, ces adresses ne peuvent pas être utilisées directement sur Internet. C'est pourquoi les routeurs de bordure des FAI sont configurés pour empêcher le routage de ces adresses.

2. Translation d'adresses

La translation d'adresse est un processus générique permettant la substitution d'une adresse par une autre, et permet ainsi de masquer les adresses privées des réseaux locaux derrière une adresse publique. Ce processus existe sous deux variantes :

- **NAT** (Network Address Translation) : statique ou dynamique
- **PAT** (Port Address Translation)

2.1. Principe du NAT

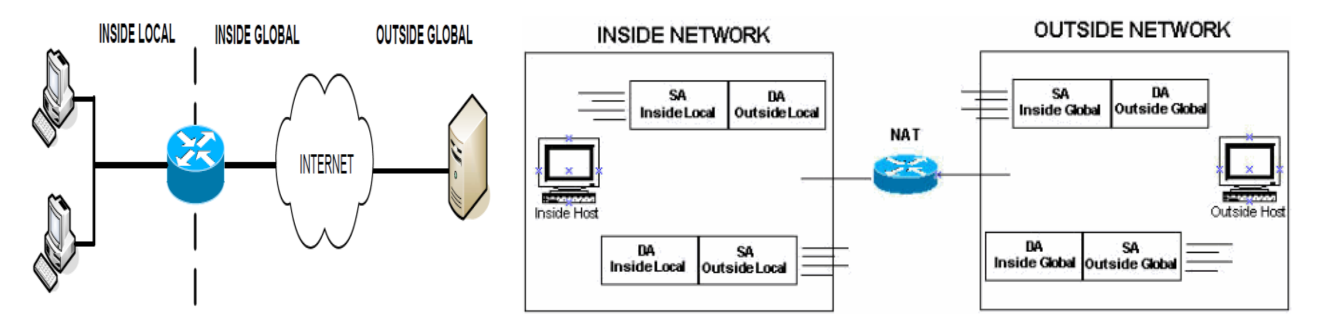
Le NAT a été fait pour économiser des adresses IP en permettant la translation d'adresses IP privées internes a une entité (une entreprise, une école, …) en une ou plusieurs adresses IP publiques routable sur Internet.
Remarque : l'adresse IP utilisée pour la translation n'est pas forcément une adresse IP publique et peut être à nouveau une adresse IP privée qui, à son tour, pourra être translatée.

Cette translation d'adresse est effectuée principalement sur les routeurs de bordure d'une entreprise connectée à Internet. Le réseau utilisant les adresses IP privées est ainsi appelé le réseau interne (inside), tandis que la partie du réseau utilisant des adresses IP publiques (Internet) est appelé le réseau externe (outside).

Quand un utilisateur du réseau interne (inside) souhaite communiquer avec un hôte du réseau externe (outside), le routeur reçoit le paquet avec l'adresse IP privée et réécrit le paquet en changeant l'adresse IP source avec l'adresse IP publique du routeur (c'est l'opération de translation).
Le routeur consulte ensuite sa table de routage pour acheminer le paquet jusqu'à la bonne destination.
Le destinataire recevra le paquet avec comme source l'adresse IP publique du routeur et non l'adresse IP privée de l'hôte qui envoie le paquet dans le réseau interne.

Au-delà des appellations « inside » et « outside », Cisco défini 4 types d'adresses pour le NAT :

- **Inside local address**
  - Adresse IP attribuée à un hôte dans le LAN.
- **Inside global address**
  - Adresse(s) IP attribuée(s) par le FAI reconnue(s) par l'Internet pour représenter le LAN.
- **Outside local address**
  - Adresse IP d'un hôte du réseau externe telle qu'elle est connue par les utilisateurs du réseau interne. La plupart du temps, celle-ci est identique à l' « outside global address ».
- **Outside global address**
  - Adresse IP attribuée à un hôte dans le réseau externe.



Le NAT peut être utilisé dans plusieurs cas, cependant il peut être configuré de deux manières différentes statiquement ou dynamiquement.

- **Le NAT statique** translate une adresse IP privée avec toujours la même adresse IP publique. S'il y a 4 utilisateurs nécessitant une translation d'adresse, il faudra donc utiliser 4 adresses IP publiques.
- **Le NAT dynamique** translate une adresse privée avec une adresse IP publique appartenant à un pool d'adresses. L'adresse IP publique utilisée pour la translation n'est donc pas toujours la même. S'il n'y a pas assez d'adresses IP publiques disponibles les utilisateurs devront attendre qu'une adresse se libère pour pouvoir être translaté.

L'avantage du NAT, en plus de la grande économie d'adresses IP, est de ne pas avoir à refaire tout l'adressage IP lorsque l'on change de fournisseur d'accès internet.
Cette technologie apporte également de la sécurité au sein du réseau interne puisque les machines qui s'y trouvent ne sont pas accessibles depuis l'extérieur.

2.2. Principe du PAT

Le PAT (Port Address Translation) ou Overloading permet d'attribuer une seule adresse IP publique pour la translation de plusieurs adresses IP privées. Chaque utilisateur est différencié grâce à un numéro de port unique qui lui est attribué lorsqu'il souhaite communiquer.
Etant donné qu'il existe 65536 ports différents, un routeur pourrait translater jusqu'à 65536 adresses IP privées différentes. Cependant en réalité, un équipement ne peut gérer en moyenne que la translation d'environ 4000 ports par adresse IP publique.

3. Configuration

3.1. Commandes

- **ip nat inside**

➢ Mode de configuration d'interface
➢ Spécifie l'interface inside.
➢ Complémentaire des autres commandes NAT

- **ip nat outside**

➢ Mode de configuration d'interface
➢ Spécifie l'interface outside
➢ Complémentaire des autres commandes NAT

- **ip nat inside source static {local-ip} {global –ip}**

➢ Mode de configuration globale
➢ Etablie une translation statique entre une 'Inside local address' et une 'Inside global address'

- **access-list {numéro} permit {prefix} {wildcard_mask}**

➢ Mode de configuration globale
➢ Spécifie le ou les réseaux autorisés à être translatés

- **ip nat inside source list {numéro} pool {nom_du_pool}**

➢ Mode de configuration globale
➢ Définie le pool qui va être translaté

- **ip nat pool {nom_du_pool} {première-ip} {dernière-ip} netmask {masque_de_sous-reseau}**

➢ Mode de configuration globale
➢ Spécifie le pool d'adresses IP : toutes les adresses IP entre première-ip et dernière-ip

- **ip nat inside source list {numéro} interface type {numéro} overload**

➢ Mode de configuration globale
➢ Configuration du PAT sur l'interface outside

- **clear ip nat translation**

➢ Mode privilégié
➢ Effacer toutes les translations dynamiques

3.2. Procédure de configuration

- Spécifier les interfaces outside et inside (ip nat outside / inside)
  - NAT statique :
    - Spécifier chaque adresse une par une (ip nat inside source static ip1 ip2)
  - NAT dynamique :
    - Spécifier le bloc privé
    - Spécifier le pool public
    - Activer le NAT avec le bloc privé et le pool public en argument.
  - PAT :
    - Spécifier le bloc privé
    - Activer le NAT sur l'interface outside avec le bloc privé en argument.

3.3. Vérification

- show ip nat translations
  - Mode privilégié
  - Affiche des informations sur chaque translation en cours.
- show ip nat statistics
  - Mode privilégié
  - Afficher des statistiques sur la translation
- show running-config
  - Mode privilégié
  - Affiche la configuration du routeur.
- debug ip nat
  - Mode privilégié
  - Affiche en temps réel toute les paquets translatés.

III. Protocole DHCP

1. Introduction

DHCP (Dynamic Host Configuration Protocol) est un protocole fonctionnant en mode Client – Serveur. Il fournit aux clients une configuration de couche 3 : principalement une adresse (IP), mais aussi des adresses de passerelle ou de serveur DNS, NETBIOS, noms de domaines, ...

Ce protocole permet une gestion dynamique de l'adressage de niveau 3. Il allège ainsi grandement les tâches de l'administrateur réseau.

Les **clients DHCP** sont fournis aux utilisateurs sur la plupart des systèmes d'exploitation. Grâce à l'envoi d'une requête au serveur, ceux-ci peuvent se voir attribuer une adresse de couche 3. Seuls les équipements utilisateurs doivent bénéficier de ce service, les serveurs et équipements réseaux devant être adressés de façon statique.

Le DHCP fonctionne sur un principe de location ou bail. Le serveur attribue une adresse à un client pour une durée prédéterminée (en jours, heures, minutes). Le client doit donc effectuer à nouveau une demande pour voir son bail reconduit.

Il existe trois types d'allocation d'adresse :

- **Automatique** : une adresse IP permanente est attribuée automatiquement au client. Un mappage statique (mac – IP) permet de retrouver la même adresse lors d'une déconnexion / reconnexion.
- **Manuelle** : l'attribution est faite manuellement par l'administrateur réseau (mappage statique). Le protocole DHCP se charge d'envoyer ces informations au client lors d'une demande.
- **Dynamique** : l'attribution se fait à la volée. Une IP libre est attribuée à un client en faisant la demande, pour une durée déterminée.

Les **serveurs DHCP** sont généralement gérés par des serveurs d'entreprise (service généralement assuré par l'OS), mais ils peuvent également être configurés sur les routeurs.

1.1. Comparatif entre BOOTP et DHCP

BOOTP (Bootstrap Protocol) est l'ancêtre du protocole DHCP. Son but était d'attribuer une configuration de couche 3 aux stations de travail fonctionnant sans disque dur. DHCP reprend plusieurs de ses caractéristiques :

- Fonctionne en mode client - serveur
- Utilise les ports UDP 67 (serveur) et 68 (client), appelés ports BOOTP
- Attribue une adresse IP
- Attribue un masque de sous-réseau
- Attribue une adresse de passerelle
- Attribue une adresse de serveur DNS

Le protocole BOOTP alloue les adresses de façon statique : le serveur BOOTP doit posséder au préalable une table de correspondance mac – IP pour attribuer une IP. BOOTP n'a pas de notion de bail et fait donc une liaison permanente entre un hôte et l'adresse IP qu'il lui donnera.
Enfin, le protocole DHCP peut fournir jusqu'à 30 options de configuration, contre 4 seulement pour BOOTP (IP, masque, adresse de passerelle, adresse du DNS).

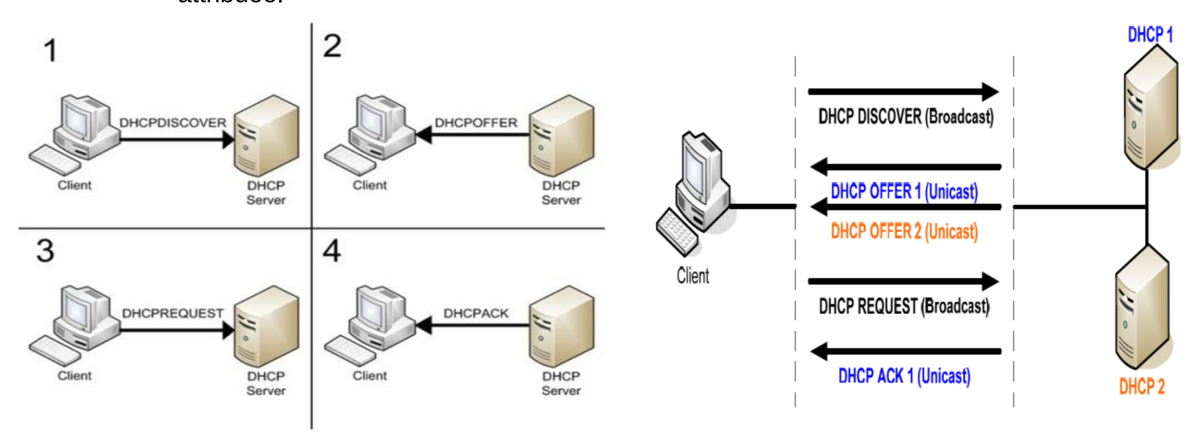
1.2. Opération DHCP

La configuration d'un client avec le protocole DHCP se fait en 4 étapes :

1) **DHCP DISCOVER** :
    - Lorsqu'une configuration DHCP cliente est présente sur un poste utilisateur, celui-ci envoie une requête en broadcast aux serveurs DHCP, appelée DHCP DISCOVER.
2) **DHCP OFFER** :
    - Les serveurs DHCP recevant le broadcast et pouvant répondre à la demande, envoient une requête en unicast au client. Ce DHCP OFFER contient toutes les informations nécessaires au client (IP, adresse de passerelle, durée du bail, serveur DNS, WINS, etc.).
3) **DHCP REQUEST** :
    - Le client émet ensuite une requête en broadcast afin de confirmer l'offre qu'il a sélectionnée (celle qui lui est arrivée en premier).
    - S'il y avait plusieurs serveurs DHCP, tous sont alors au courant et peuvent libérer leur offre en conséquence.
    - S'il s'agit d'un renouvellement de bail, le client propose au serveur l'IP qu'il veut se voir réattribuer.

4) **DHCP ACK** :

- Cette confirmation est envoyée en unicast par le serveur DHCP au client. Une fois le DHCP ACK reçu, le client peut alors utiliser l'adresse IP ainsi que le reste de la configuration attribuée.



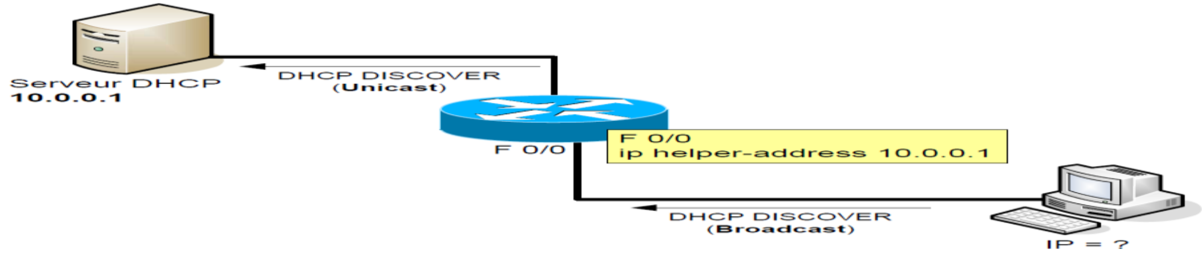
Il existe trois autres requêtes DHCP :

- **DHCP DECLINE** : Si le client détecte l'IP qu'on lui a proposée sur le même segment réseau, il envoie cette requête au serveur. Le processus redémarre alors.
- **DHCP NACK** : Lorsqu'un serveur détecte que l'IP pour laquelle il doit renvoyer un ACK est déjà présente sur le réseau, il envoie un DHCP NACK. Le processus doit alors redémarrer pour le client concerné.
- **DHCP RELEASE** : Lorsqu'un client veut annuler le bail (arrêt du système, commande ipconfig /release sous Windows), cette requête est envoyée au serveur afin qu'il libère la réservation d'adresse.

1.3. Relais DHCP

Les serveurs DHCP font partie des serveurs d'entreprise. Il est très courant que ces serveurs soient placés sur un sous-réseau différent de celui des utilisateurs.
Un problème se pose donc : les requêtes clientes étant envoyées au serveur DHCP en broadcast, un routeur segmentant le réseau arrêtera également ces broadcast. Il en va de même pour les services DNS, TFTP, TACACS (service d'authentification), etc.
Il est possible d'éviter ce problème en appliquant la commande ip helper-address sur l'interface d'un routeur. Celle-ci permet de relayer les broadcast UDP vers une adresse unicast définie. Ce relais se fait au niveau des services UDP suivants :

- Protocole Time
- TACACS
- Le protocole DNS
- Le service BOOTP/DHCP
- TFTP
- Le service NetBIOS



2. Configuration

Comme pour le NAT, la configuration DHCP nécessite la définition de groupe(s) de plages d'adresses attribuables.

2.1. Commandes

- **ip dhcp pool {nom_groupe}**

➢ Mode de configuration globale
➢ Passe en mode de configuration DHCP
➢ Spécifie et nomme un groupe d'adresses

- **ip dhcp excluded-address {prefix} [prefix2]**

➢ Mode de configuration globale
➢ Spécifie l'adresse ou la plage d'adresses à exclure du DHCP

- **[no] service dhcp**

➢ Mode de configuration globale
➢ Active/désactive le service DHCP
➢ Actif par défaut

- **network {prefix} {masque}**

➢ Mode de configuration DHCP
➢ Spécifie la plage d'adresses attribuables

- **default-router {prefix}**

➢ Mode de configuration DHCP
➢ Spécifie la passerelle par défaut

- **dns-server {prefix} [prefix2, prefix3, ...]**

➢ Mode de configuration DHCP
➢ Spécifie le(s) serveur(s) DNS

- **netbios-name-server {prefix}**

➢ Mode de configuration DHCP
➢ Spécifie l'adresse du serveur NETBIOS WINS

- **domain-name {nom}**

➢ Mode de configuration DHCP
➢ Spécifie le nom du domaine

- **lease {infinite | jours [heures] [minutes]}**

➢ Mode de configuration DHCP
➢ Spécifie la durée du bail
➢ Valeur par défaut : 1 jour

- **ip helper-address {prefix}**

➢ Mode de configuration d'interface
➢ Relaye les broadcast UDP (requs sur l'interface) vers l'adresse unicast spécifiée.

2.2. Procédure de configuration

Voici la procédure permettant de configurer le service DHCP sur un routeur Cisco :

- Définir le nom du groupe d'adresses (commande ip dhcp pool)
- Définir les plages d'adresses attribuables (commande network)
- Spécifier la passerelle par défaut (commande default-router)
- Exclure les adresses IP statiques (commande ip dhcp excluded-address)

Commandes optionnelles :

- Spécifier l'adresse du serveur DNS (commande dns-server)
- Spécifier la durée du bail (commande lease)
- Spécifier l'adresse du serveur NETBIOS (commande netbios-name-server)
- Spécifier le nom de domaine (commande domain-name)
- Relayer les broadcast vers le serveur concerné (commande ip helper-address)

2.3. Vérification

Deux commandes show permettent de vérifier le bon fonctionnement du protocole DHCP :

- show ip dhcp binding

- Mode privilégié
- Affiche les liaisons créées par DHCP (mac – IP)
- Affiche la date de fin du bail
- Affiche le type d'allocation d'adresse (Automatique, Manuel, Dynamique)

- show ip dhcp server statistics

- Mode privilégié
- Affiche les requêtes DHCP envoyées et reçues.